Trust, Identity, Privacy, and Security Considerations For Designing a Peer Data Sharing Platform Between People Living With HIV

ADRIAN BUSSONE, Centre for HCI Design, City, University of London, London, United Kingdom
BAKITA KASADHA, Terrence Higgins Trust, London, United Kingdom
SIMONE STUMPF, Centre for HCI Design, City, University of London, London, United Kingdom
ABIGAIL C. DURRANT, Open Lab, Newcastle University, Newcastle upon Tyne, United Kingdom
SHEMA TARIQ, Institute for Global Health, University College London, London, United Kingdom
JO GIBBS, Institute for Global Health, University College London, London, United Kingdom
KAREN C. LLOYD, Institute for Global Health, University College London, London, United Kingdom
JON BIRD, Department of Computer Science, University of Bristol, Bristol, United Kingdom

ABSTRACT

Resulting from treatment advances, the Human Immunodeficiency Virus (HIV) is now a long-term condition, and digital solutions are being developed to support people living with HIV in self-management. Sharing their health data with their peers may support self-management, but the trust, identity, privacy and security (TIPS) considerations of people living with HIV remain underexplored. Working with a peer researcher who is expert in the lived experience of HIV, we interviewed 26 people living with HIV in the United Kingdom (UK) to investigate how to design a peer data sharing platform. We also conducted rating activities with participants to capture their attitudes towards sharing personal data. Our mixed methods study showed that participants were highly sophisticated in their understanding of trust and in their requirements for robust privacy and security. They indicated willingness to share digital identity attributes, including gender, age, medical history, health and well-being data, but not details that could reveal their personal identity. Participants called for TIPS measures to foster and to sustain responsible data sharing within their community. These findings can inform the development of trustworthy and secure digital platforms that enable people living with HIV to share data with their peers and provide insights for researchers who wish to facilitate data sharing in other communities with stigmatised health conditions.

CCS CONCEPTS

• Human-centered computing~Human computer interaction (HCI) • **Security and privacy~Social aspects of security and privacy**

KEYWORDS

Data sharing, HIV, health data, trust, identity, privacy security

ACM Reference format:

Adrian Bussone, Bakita Kasadha, Simone Stumpf, Abigail C. Durrant, Shema Tariq, Jo Gibbs, Karen C. Lloyd and Jon Bird5. 2020. Trust, Identity, Privacy, and Security Considerations For Designing a Peer Data Sharing Platform Between People Living With HIV. *Proc. ACM Hum.-Comput. Interact.* 4, 173. 2 (October 2020), 22 pages. https://doi.org/10.1145/3415244

1 Introduction

The Human Immunodeficiency Virus (HIV) affects over 37 million people worldwide [71]. What was once a life-limiting illness is now a long-term condition managed with antiretroviral drugs (ARVs). However, living well with HIV requires careful self-management, which can be particularly challenging when dealing with side-effects of ARVs and complications linked to a weakened immune system [21]. For example, a woman living with HIV who suddenly experiences night sweats, poor sleep and irregular menstruation, is left to determine if these changes are ARV side effects, a symptom of another HIV-associated condition such as tuberculosis, or the start of menopause [64].

There has been rising interest in the design and use of digital technology amongst people living with a range of health conditions to support self-management [28,31–33,70]. A large proportion of the research in Computer-Supported Collaborative Work (CSCW) and Human-Computer Interaction (HCI) has focused on the informational, emotional and social support provided through online forums and social networking sites, in which people living with a condition can share their experiences and expertise with their peers [16,23,27–29,44,49,50,56,70]. This focus on mutual support amongst peers is also mirrored in research focusing on people with HIV, which has shown that people with HIV look for information and advice about their health from a variety of sources, including newsletters, magazines, personal physicians, and friends [26,46–48,62,63,66]. Remaining underexplored is the use of digital collaborative technologies to share and exchange health data; most research in this area has investigated the exchange and use of health data as part of electronic patient health records (ePHRs) between patient and healthcare professionals [10,53,69]. However, in the absence of frequent healthcare consultations, people living with HIV and other chronic diseases are tracking and storing personal health data to record their lab results, medication adherence, symptoms, side effects, and other activities and experiences, in a variety of ways [7,20,24,36,55,57]. It has been argued that reflecting on one's own health data using digital technologies is important for self-management, especially when there are fluctuations in health[45]. However, research indicates that individuals reflecting on personal health data by themselves may not always result in acquiring new knowledge [54]. Yet current digital technologies for personal health data are predominantly focused on individual use, rarely supporting users in sharing and viewing the health data of others [52]. Hence, this self-tracked personal health data is frequently shared with peers haphazardly in online forums [8,54] in order to determine if their personal health data was typical, or 'normal', for someone with that condition [54], or they sought input from others to try to understand their personal health data [8].

A novel area for research is how people living with a range of long-term conditions can track and share their personal health data with their peers using digital technology specifically designed for this purpose. So far there are very few technologies that support this. The most well-known web application for tracking health information is *Patients Like Me* (www.patientslikeme.com/) [18,69], which can be used to log emotional changes, physical changes, and lab results, and then share aggregated data with others using the same platform. There are few technologies dedicated to allowing people living with HIV to track their data [5,38,72], and to our knowledge, none that allow sharing of these data with their peers.

However, sharing personal health data with others is not without its risks. Those who do so risk both the privacy and security of their personal data, increasing the chances for inappropriate access, misuse, and wrongful disclosure [41,67]. Therefore, trust, identity, privacy and security (TIPS) considerations play an important part in the adoption and continued use of health-focused technology and data sharing platforms [6,10,16,22,34,43,50,53,56,69]. In our work, we employ concepts common in TIPS research, adopted from a privacy and security perspective. Online networks are made up of *entities* – that is, a person, group, organisation. Users will have a *personal identity* in real life plus one or more *digital identities* that provide access to and use of systems [15,58]. In contrast to notions of identity commonly used within CSCW arising from identity theory and social identity theory [25], we use the term 'identity' to mean identifiers that are

associated with a person in order to authenticate themselves and interact with systems, services and processes, either in the physical or digital world. Personal identity in the physical world might comprise a name whereas a digital identity is usually concerned with usernames and digital account details. Digital identities comprise and store one or more attributes, such as personal data, or medical records.

To share data between entities, there needs to be some trust. We view *trust* as a social tie between two parties, in which one opens themselves up to vulnerability by sharing something with the other, with the expectation that the other party will behave appropriately[65]. Privacy and security are important aspects for trust, where *privacy* concerns a person's ability to choose how their data are revealed to others [1,4,68] while *security* refers to the safety of a person's data and protection against unwanted access [1,7]. We connect with mature debates about the conceptualisation of *online privacy*, which frame problems related to users' perceived sense of *security in digital spaces*, for example, how such 'spaces' may be defined by technological mechanisms, how flows of personal information may permitted, or constrained by norms, and how informed consent models depend on notions of transparency and control that may not be real [51]. Establishing the genuine trustworthiness, or credibility, of a digital application (app) is non-trivial given the complexity of digital connections [60]. Significant challenges remain for digital technology designers to implement *secure and trusted systems* for delivering *privacy and digital identity management.*

So far the TIPS considerations of people living with HIV for sharing health data with peers remain underexplored. This research gap must be addressed if we are to build effective and acceptable digital tools for health data sharing to support people living with HIV to better understand and self-manage their health. Our findings also hold lessons for building solutions for people living with other stigmatised diseases in which privacy and security of shared data are of importance to users.

The work we present here is part of the larger 'Interaction Design for Trusted Sharing of Personal Health Data to Live Well with HIV' (INTUIT) research project aiming to co-design a digital platform to enable trusted, private and secure health data sharing in a range of settings, such as between patients and healthcare professionals, between peers and between people living with HIV and third party organisations. This research project involves a collaborative research partnership with a UK HIV organisation, the Terrence Higgins Trust, that employed a peer researcher [30]who is an expert in the lived experience of HIV. The peer researcher was involved in designing and conducting the study and is a co-author of this paper.

The study reported on herein investigated the TIPS considerations that people living with HIV make when sharing data with each other. We worked in close cooperation with a community organization, the Terrence Higgins Trust, which employed a peer researcher – a researcher living with HIV. We interviewed 26 people living with HIV living in the UK to understand their TIPS concerns about sharing data with their peers. Our research questions were:

1. How do people living with HIV conceptualise trust, privacy and security for sharing data with others? How familiar are they with these concepts in relation to digital tools?

2. What attributes of their digital identity are people living with HIV willing to share with other entities? What data are especially sensitive and private?
3. What trust, identity, privacy and security considerations do people living with HIV make when sharing data with peers? What are the implications for designing digital technologies for sharing personal health data amongst peers?

In this paper we report on the findings from our investigation, addressing the above research questions to deliver three main contributions to the CSCW literature on TIPS:

- A better understanding of the trust, privacy and security needs of people living with HIV when sharing health data among peers;
- Design considerations for the development of digital tools that facilitate sharing of health data for people with HIV with their peers;
- Insights for researchers and designers who wish to facilitate data sharing in other stigmatised health communities.

2 RELATED WORK

2.1 Digital Tools For Tracking and Sharing Personal Health Data

It is becoming increasingly common for people living with health conditions to track data about themselves and their health for self-management [17,45] through mobile apps, websites, etc. [20,36]. The health data that these tools facilitate users in tracking must be relevant to that user's health concern or condition [40]. For people living with HIV, this means tracking and monitoring a range of data, such as weight, exercise, emotions, lab results, other health conditions, side effects or symptoms [7,14,59]. However, there are very few digital systems designed specifically for people living with HIV to track and monitor their health. TIDES [38], an application developed by academic researchers, is designed to provide targeted interventions to HIV+ people to support self-care and avoid depression. A website called myHIV [72], which was developed by the Terrence Higgins Trust (THT), a HIV and sexual health charity in the UK, allows users to set up medication and appointment reminders, log their laboratory results, and record notes about side effects they have experienced. BeYou+, is a mobile phone app [5] that allows users to track their laboratory results, medication, and appointments. Finally, the EmERGE project seeks to develop an mHealth platform to facilitate self-management and communication between those living with HIV and their healthcare team [46].

Many people informally share and exchange the personal health data they have tracked with their peers on social networking sites or online health communities as a means to understand, manage, and make decisions about their health [8,13,54]. Work is starting to emerge to support sharing and exchanging health data formally [9,18], for example, the online health network PatientsLikeMe allows individuals to share their tracked health data with all other users [18,69]. To our knowledge, there is currently no platform specially for people living with HIV to share their health data with their peers in a trusted, private and secure manner.

2.2 Trust, Identity, Privacy and Security (TIPS)

Sharing health data with peers online can be risky [41,67]. Doing so can jeopardise the privacy and security of one's personal and digital identity and data, increasing the chances for inappropriate access, misuse, and wrongful disclosure [18]. Furthermore, a breach in privacy or security might lead to loss of trust in sharing data, and might make users abandon a digital platform [42]. Unfortunately, previous research has shown that such users may not always pay attention to the privacy and security provisions of a digital platform [42,61]. Instead, they often informally assess a digital platform to determine their trust through reputation and credibility. For example, platforms hosted by commercial entities may be seen as biased and self-serving, while charities or non-profit hosts are likely to be viewed more positively [3]. Also, privacy seems

to be managed in complex ways by individuals; users of online systems may prefer to share very *sensitive* data with peers at a greater social distance[12] while sharing data considered *personal* (e.g. their marital status, family status, or the area they live in) with those to whom they have closer social ties [19]. In such scenarios, users are typically making choices to share personal data through well-defined digital spaces to which access can be controlled – such control can be critical for the trustworthiness of these tools, but challenging to implement [51,60].
Thus, there is a need for online collaborative tools that support people living with long-term conditions in sharing their data with their peers, and such tools must be appropriately designed in line with the TIPS considerations of the target users. TIPS considerations are absolutely vital to investigate in the design of health data sharing platforms [6,10,16,22,34,43,50,53,56,69], particularly for people living with stigmatised conditions, like HIV, as lack of privacy and security of their digital identities and data attributes could expose individuals' personal identities in the physical world, leaving them vulnerable to abuse or discrimination.

3 Method

We adopted a mixed-methods approach, conducting semi-structured interviews with people living with HIV, coupled with rating activities to capture their attitudes towards sharing attributes of their digital identity. This allowed us to analyse the ratings quantitatively, and supplement our understanding through qualitative analysis of the interviews. The peer researcher involved in this project informed the choice of methods, in particular for sampling and recruitment, and the use of language to support participant engagement with the study.

3.1 Participants

We recruited 26 English-speaking individuals; all adults (≥18 years) living with HIV from around the UK who were interested in the development of a digital system for sharing their health data with their peers. Participants were given a £20 Amazon gift voucher in recognition of their time. There were 11 women (10 cis[1]) and 15 men (14 cis), aged 20 to 63 (mean 44.3, median 46.5). Out of the 26 participants, 17 identified as heterosexual, 7 as homosexual, 1 as bisexual and 1 as queer. For detailed demographic details please see Appendix A.1. Five of the participants had acquired HIV at birth (perinatally), and five were considered 'long term diagnosed' (receiving their diagnosis before 1996); duration of diagnosis ranged from 4 months to 33 years (mean of 14 years). Many of our participants reported that they used online forums or support websites to ask questions or provide support to other people living with HIV. A small number acted as peer counsellors online.
Recruitment adverts were distributed through sexual health organisations, social media, and WhatsApp groups, facilitated by the peer researcher. The ethics of this study were considered extensively, and it was approved by the Computer Science Research Ethics Committee, City,

[1] 'Cis' or 'cisgender' refers to a person whose sense of personal identity and gender corresponds with the sex they were assigned at birth

University of London. Once a potential participant contacted us, they were sent information about the study and a consent form via email to review. All those recruited into the study were assigned a unique identification number on receiving consent. Audio data were stored in an encrypted folder on the researcher's computer until they were transcribed in full. Once this was done, audio files were destroyed. All transcripts were examined for identifiable data, which were then permanently redacted. All personally identifiable data of participants were deleted.

3.2 Procedure

Interviews were conducted by the first and second author, the peer researcher. At least one of the researchers were present, using a discussion guide to structure the conversation. Before the interview started, each participant was asked to complete a demographic questionnaire, using categories previously employed in other HIV research [7,37]. Once this was completed, the interview session began, each lasting approximately 90 minutes. We began by asking participants to recall instances in which they shared personal health data with peers, or vice versa. We then probed participants' understandings of trust, privacy and security. Following this, participants were asked to imagine a new online platform where they could track and share their data with peers; they were then guided through a series of questions exploring their TIPS considerations when sharing their data with different entities: where their data are stored (the 'host platform'), who has access to their data as part of their peer group ('community'), and sharing data with individuals in the community ('community members'). In the interviews, we referred to Community as "a community of people who are living with HIV" and community members as "individuals in that community who you can decide to share information with, and maybe they with you".

For each of these entities (i.e. host platform, community, and community members) of the envisioned system, participants were asked to rate how comfortable they would feel in sharing particular identity attributes to investigate their data privacy requirements (Figure 1), using a Visual Analog Scale method often used in medical domains e.g. [39]. Small slips of paper were prepared, each describing different pieces of data (e.g. "my name", "my gender," "my email address"). These data items are attributes associated with digital identities, and are often tracked and shared by people living with HIV [7,8]. The items they rated represented three types of data: *personal data*, e.g. name, age, gender, *medical data*, e.g. date of diagnosis, medication, CD4 count and viral load, and *lifestyle data*, e.g. exercise and weight. Participants could add further data items as required. Three new data items (hobbies, sexual activity, menstruation) were added but were excluded from the analysis because each was only created by one participant. These slips were then placed by participants on a sheet of paper along a spectrum of "very uncomfortable" to "very comfortable", and we asked participants to 'think aloud' as they placed the data item.

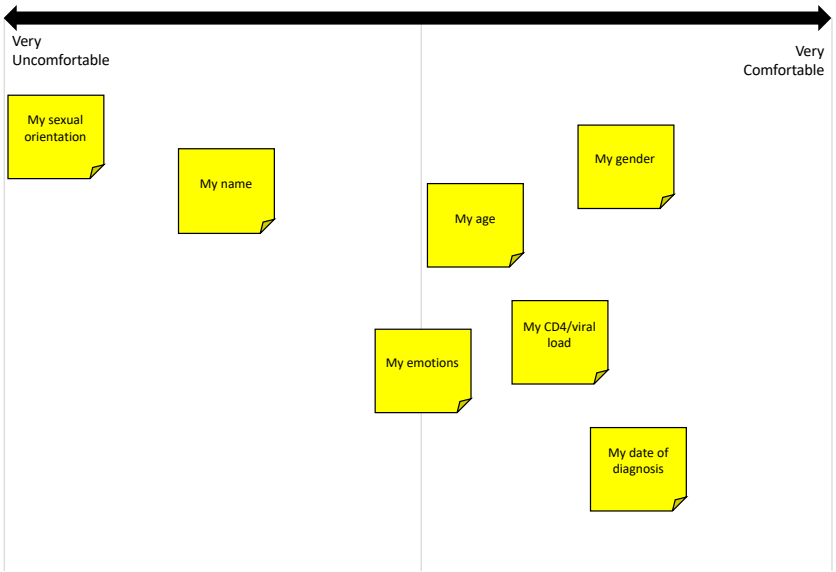

Fig. 1. Slips with data items were placed by participants on a sheet with a rating scale between 'very uncomfortable' to 'very comfortable'. This indicated how they felt about sharing these data items with other entities.

3.3 Data Collection and Analysis

Each interview session was audio-recorded and transcribed. We analysed the interview data thematically [2], first developing a coding scheme for participants' understanding of trust, privacy and security (RQ1), then developing one for their TIPS considerations across the entities they interacted with (RQ3). Both these coding schemes can be found in the appendix A.2. To ensure reliability of the coding, we calculated the Jaccard Index for two independent coders on 20% of the data for both coding schemes. Agreement ranged between 0.67 and 1.00 for codes which is within an acceptable range. We highlight the themes and insights we report on in bold, and support the account of our thematic analysis by providing quotes to give salience to individual participants' voices. In doing so, we foreground how each person made sense of TIPS concerns in their own way, and how their perceptions and use of data were shaped by contextual factors – a point we return to later in the paper.

To analyse participant ratings for data privacy (RQ2), we measured the distance from the left-most line (very uncomfortable) to the middle of each slip of paper. To account for potential differences in paper sizing and units of measurement, we normalised the measurement to be between 0 and 100. For example, a slip of paper placed exactly on the 'very uncomfortable' line was 0, whereas a slip placed 27 cm from the left would be scaled to 77 on a 35cm scale. The nature

of the data we collected allowed us to investigate privacy requirements statistically. We conducted Repeated Measures ANOVA tests, followed by post-hoc analyses, to identify statistically significant differences between data items and between entities. We turned to the transcripts to explore reasons participants gave for their ratings.

4 Results

We first investigated how familiar people were with aspects of trust, privacy and security in relation to their personal and digital identities and other entities in online settings. This allowed us to study important themes in general TIPS considerations of people living with HIV, that matter to the design of data sharing platforms. We then turned our attention to investigating what data people with HIV considered sensitive, and might want to keep private. Finally, we analysed in detail specific requirements for data sharing platforms among peers living with HIV.

4.1 How People Living With HIV Understand Trust, Privacy and Security (RQ1)

Recall that common formal definitions were:

- Online networks are made up of *entities*, such as a person, group, or organisation.
- Users will have a *personal identity* in the physical world and one or more *digital identities* that provide access to and use of systems.
- *Trust* as a social tie between two parties, in which one party opens themselves up to vulnerability by sharing something with the other party with the expectation that the other party will behave appropriately.
- *Privacy* concerns a person's ability to choose how their data are revealed to others, while *security* refers to the safety of a person's data and protection against unwanted access.

In contrast to some previous research in online privacy and security [42,61], we found that almost all of our participants had a very good understanding of trust, privacy and security that aligned with the above definitions. Up to two-thirds of the 26 participants were able to define these concepts very easily, with trust matching the above definition most frequently and privacy least frequently.

4.1.1 How Is Trust Established and Maintained?. Participants frequently considered **characteristics of trusted individuals or organisations** for establishing and maintaining trust. Most of the participants felt that personally knowing the trustee, i.e. the other entity in which trust is placed, was important, and expressed concerns regarding trust when sharing 'everything' with 'everyone':

> "If I'm talking to a stranger, I don't know that person. It's not a relative, it is not a professional, it is someone I just met, I can't trust [them] because I don't know what that person is going to use [the information for]." – P25

Some participants referred specifically to their trust in digital systems, professionals or organisations. Five of the participants talked about placing trust in a digital system, e.g. a specific platform such as Terrence Higgins Trust's myHIV site, or a centralised system like medical records kept by the NHS. Similarly, medical professionals, researchers, and HIV or health-related organisations were mentioned as parties that could be trusted.

Participants reported that, within the trusted relationship, it was just as important to know what the trustee was going to do with the data: trust was shaped by participants' **expectations of the trusted entity's behaviour**. The core concern was that data were kept confidential and safe, as expressed by 15 participants, showing that **privacy and security** are important considerations in participants' trust of others. A different facet of participants' confidence in others, mentioned by nine participants, was what the trusted entity would do with that information. It was important to them that the trusted entity would act as had been agreed, and in their best interests:

> "So say if it was a medical professional. [...] I trust that you have my best interests at heart, you're gonna do what's right to me medically." – P03

These extracts reflect a sense of trust in the assumed behaviour of the trusted entity; if that entity's role is known, e.g. being a professional versus a stranger, possibly reflected in their digital identity, this may foster confidence and trust, as it may be easier to assume that their data will be treated with care and respect.

4.1.2 What Is Key in Privacy and Security Considerations?. While eight participants talked about privacy in vague terms, the remainder defined it in terms of disclosure and choice over what to share. The majority of participants emphasised the importance of being able to choose what data to share, especially **sensitive data**:

> "When it comes to the more sensitive matters, like how I contracted HIV – my story – that's sensitive to me, which I'd expect more privacy in." – P18
> "It all depends what's... If it's medical stuff, I'm alright. If it's my HIV, I'm alright. But if it's dating, I would like some privacy." – P12

Nine of our participants differentiated between **public and private domains**, with consequent impacts on how they may choose to share data; in general, they indicated that they make very considered choices what to expose publicly or what to keep private.
Particularly contentious were data that could lead to their **personal identity** being revealed; it was important to have control over these data items and how they were 'passed on':

> "The option to opt out if you don't want to share that information. You know, gender, status, age, the usual stuff. Your basic identity details." – P01

Security of data was sometimes equated by participants with trust and privacy, and closely aligned with retaining personal control over what is shared and how. However, 17 out of 26 participants spoke of protecting their data from unauthorised access, drawing on lock and key metaphors, to **prevent disclosure or unwanted access** that might compromise their personal safety and lead to emotional harm:

> "In terms of HIV, I associate security with safety. When I think of security, I think of safety as well. No harm from what I say. I mean, emotional harm. That's how I take it." – P25

4.2 Participants' Data Privacy (RQ2)

After understanding the TIPS background for people living with HIV, we turned our focus to how their general privacy considerations expressed themselves through specific data items – this allows us to study which data items are particularly sensitive to people living with HIV, and which ones they usually have less qualms about sharing. Using the rating activities, we asked participants to indicate how 'comfortable' they would feel in sharing their data with three entities: adding it to a host platform, sharing it with a community, and sharing it with specific community

members. Figure 2 shows the mean ratings on each data item across these entities.

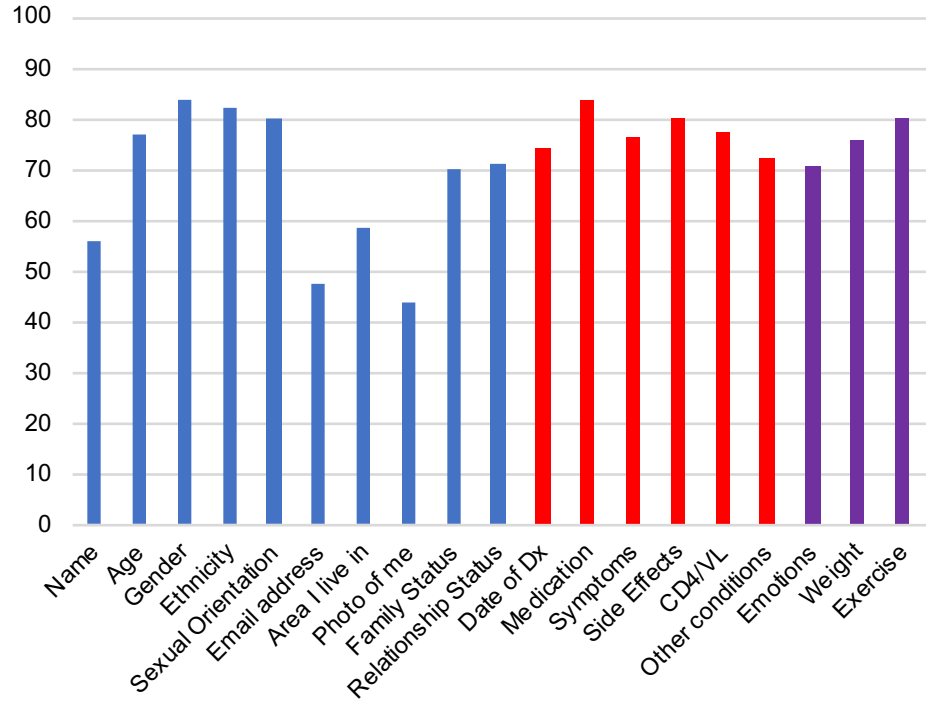

Fig. 2. Mean ratings for data items across entities. Personal data is shown in blue, medical data is shown in red, and lifestyle data is shown in purple. A rating of 0 indicates very uncomfortable sharing this data item, 100 indicates very comfortable sharing this data item.

The ratings show that participants were largely **open to sharing a wide array of data types**. Challenging our assumptions, participants were found to be as comfortable sharing personal data as they were medical data. There were several outliers in the ratings, revealing that some people were hesitant to share personal data such as ethnicity, medical data such as medication, side effects and CD4 count, or lifestyle data such as emotions. For example, two participants were unwilling to share their sexual orientation because they viewed this as irrelevant to their health journey, but also expressed fears that sharing these data might lead to prejudice and stigma:

> "Because, right, you could be talking to someone. And then suddenly they find out that like, you're bi or something, and then all of a sudden, they're like, 'Oh, you're bi, I thought you were this, I hate bi people.' You know how it is, like people just judge. And I kind of like, like, you need to work out where an individual is on their level of acceptance for these things. Because otherwise, it's just opening you to potential abuse." - P07

Participants' ratings were linked to the perceived benefits of tracking and sharing data. Our participants explained that sharing these data types **support communication with healthcare professionals**, **build community** and **enhance their own learning and self-monitoring**:

> "The good thing is that [with a system to track and share] I can remember everything to ask the doctor. So if you read about it, then you can go to a doctor and say, you know, I understand this. And then you get knowledge, knowledge is power." – P15
> "By giving people information, or putting information in the hands of the people, there's more power and more possibility to achieve change of any kind. [...] For me, it's that sense of building community." – P05

> "Being more aware about myself. Feeling like I can learn from the app. [...] If, say, I did struggle with adherence, and it is that ability to kind of have accountability and stuff like that." – P16

However, many of our participants confirmed that they would feel **less comfortable sharing data that may reveal their personal identity**, whether accidentally or deliberately, as already hinted at as a key concern in section 4.1.2. As can be seen in Figure 2, ratings for sharing name, email address, 'area lived in', and 'photo of me' were rated significantly lower than all other data items. A repeated-measures ANOVA between all data item ratings within each entity, followed by post-hoc tests, confirmed this pattern for the host $F(6,153) = 6.886$, $p<0.0001$, for community $F(6,147) = 13.338$, $p<0.0001$, and community members $F(6,152) = 8.522$, $p<0.0001$). These items often make up a 'profile' on other platforms, however, participants in our study were especially concerned that these data could be used by the community and community members to identify individuals and give clues to their personal identity in the physical world, especially when combined with 'area lived in'. The potential of using a combination of data items to reveal the personal identity was particularly unwelcome to participants who did not reside in London, who felt that sharing this could make them more easily identifiable as there would be fewer people that matched a profile.

However, participants felt less concerned about sharing some data with the host platform, such as name and email, than with others. This is likely due to previous experience with other platforms in which these items are used for account logins and to confirm their digital identity. In addition, it also seems that they trusted the host platform to keep these items secure and private, as previously highlighted in section 4.1.1.

4.3 Participants' TIPS Considerations For Sharing Data (RQ3)

In order to design platforms that allow people living with HIV to share data with their peers, it is important to understand their sensitivities and requirements. In particular, we wanted to explore in detail how they assess trust in entities they encounter as part of this platform, how they wanted to protect their personal and digital identities, and the data associated with them, and how the sharing of data between peers could be better facilitated. The following main themes emerged as important when sharing data with peers on a digital platform: reputation indicators, privacy features, security features, rules of interacting and fostering the sharing of data.

4.3.1 Reputation Indicators. To establish trust in an entity when sharing data, 22 participants indicated that they used a range of reputation indicators to ascertain the credibility of either the host platform, the community in which to participate, or individual community members. To determine if a platform was trustworthy, participants valued **aesthetics** and **usability**: platforms should look clean, have a nice typeface (*"Can't be out here having Comic Sans." – P11),* and pay attention to good information architecture and appropriate terminology (*"It should be something easy. Not cumbersome. Because we spend a lot of time on computers and with this, even though it is to do with our health you don't want to spend too much time. Simple, simple language." – P21).* This reflects previous research suggesting these as factors in fostering trust in health websites [3].

The **reputation and size of the organisation** that created or endorsed the platform was also stated as an important component of trust. Small organisations were not trusted to have the power or money to create a secure and private platform, whereas larger national organisations such as THT or the NHS were seen as more credible:

> "I cannot trust small individual companies with my information. I want big organisations, not the amateurs. [...] but if it was tied to the NHS or Terrence Higgins Trust it's a little more trustworthy." – P02

Ten of the participants described how they would determine if the community on the platform was credible and trustworthy. Their responses related mostly to how the community engaged and interacted online. For example, some expected to see **objective and balanced exchanges** that built cohesion and feelings of belonging, or that offered practical support, sharing only facts or experience-based opinions within the community.

Although most participants were unwilling to share names, some recognised that **personal details** could foster trust between individual community members. In the absence of being able to meet community members in person, their online identity was also seen as a reputation indicator. In this case, it was important for participants to be able to review users' personal and medical data, their online activity, and possible bandwagon cues [35] that indicate the popularity of their contributions (e.g. star ratings, likes, hearts, etc.) on the platform before deciding to engage:

> "Somebody will come along and agree with him, like, I will refer back to the Terrence Higgins [myHIV] thing, because that's my way of experience of this set of things. There's a thank button. So you can thank somebody for their post. So you get to trust people, and especially because the people that you know that you can trust have essentially 'liked' that comment. So you can go 'Right. Okay, that's trustworthy. It's not fake news.'" – P17

4.3.2 Privacy Features. Research in peer sharing within cancer communities has indicated that users do not necessarily pay much attention to the privacy policies of the platform [42]. In contrast, many of our participants expected a platform to include a **privacy policy** that they could read in detail, in order to determine if the platform was trustworthy.

As has been highlighted in previous research in online communities [16,50,56,69], data privacy is important for sharing among peers. Our participants described various personal strategies for maintaining their privacy and remaining in control of sharing their HIV status and data, to avoid accidental disclosure. For example, 16 indicated that an app showing a red ribbon icon or labels that say 'HIV' would be unacceptable. Nearly half expressed a preference for **sophisticated privacy controls**, in order to set what data to share, how and with whom:

> "So there would be serious limits on personal stuff, and, and anything that could identify me, but it would be good to have a choice to change that at a later date. Again, for somebody like me, newly diagnosed. To me, it's locked down. It's my choice as to who I share it with. But yeah, I think as long as I have complete control over what parts I could share, yeah. That would be important." – P01

This also extended to the length of time data is shared:

> "People's circumstances change. So taking back your shares... it's easy to make the decision, but you want it equally as easy to undo it." – P01

Some participants suggested platform features to **prevent other individuals from keeping data**, through preventing screenshots, or only allowing data to be viewed for a short period, e.g. 48 hours.

Participants placed great importance on avoiding sharing data that would divulge their personal identity, as previously highlighted by their relative unwillingness to share their personal data (see section 4.2):

> "I would expect that you wouldn't necessarily have to share your name or whatever. I'm not sure how you would register without your name. But I would only say that some people wouldn't even feel that comfortable. And so I would expect for there to be options to be able to say, 'No, this is supposed to benefit me. So I get to decide how much I get to share about myself.' – P16

4.3.3 Security Features. More than half of our participants stated a need for strong security, akin to the level established in banking, in order to protect their data. Transparency of security arrangements was key, and 13 of our participants showed a keenness to know the details of **security policies**. Some were highly nuanced in their understanding of security features to ensure secure data transmission, including SSL and TSL certificates.
A **secure login** process, mentioned by 13 participants, was also prized. They discussed processes to ensure this, including pin codes, passwords, security questions, two-step verification, and automatic logouts:

> "That thing that logs you out. So if you look, for example, on my phone, my HSBC app, I can be on there. And then let's say I get on to another app , I won't then be able to get back on my HSBC app without either putting my fingerprint or going through a security check for me to let me back in, even though I've literally just left it for two seconds. So that will make me feel more like no one else can come on my phone and be me, or no one else can access what I have. Apart from me." – P09

Participants were clear in their expectations that systems should include an **identity verification process**, to ensure that only those living with HIV could use it. This was raised by 18 of our participants:

> "That verification process would give me an assurance, like this person's been verified or they've gone through the process of… Because you don't want it to be like social media where anyone can sign up, and it's like a free world you come in, you can make your own identity etc. This is to do with people's actual health and something that's really close to close to them. So yeah, I think that verification process is key, because it just authenticates that person, whether they want to share their name or is up to them but the fact that they are there only for me to be assured that they are going through or have the same experience in some ways, as I do. And that's what I'd be looking for on the platform." – P18

Various methods of verification were suggested, including a code from a healthcare professional, an HIV clinic, or a trusted HIV-related organisation, which could then be used to sign up.
4.3.4 Rules of Interacting. Many participants described attending face-to-face HIV support groups, where **rules of behaviour** are explicitly stated, such as respecting what people say and not disclosing what is said beyond the confines of the support group. Such rules of behaviour were viewed as being equally important online; of the 26 participants interviewed, 20 referred to appropriate ways of interacting or engaging, having administrators or moderators in place, and

there being repercussions for breaking the rules. Participants felt that these rules should be clearly outlined from the outset. However, it was also felt that the rules should be set by the community, reflecting its values as they evolve and change:

> "I'd expect there to be values that we all share. But also values that we are committed to. If there was something like a yearly review where people got to send in like 'This would be cool. This would be cool' and thinking about introspectively, about what works and what hasn't worked. [...] You know, obviously it's a new thing so it's not going to be perfect. So you'd want the chance to be able to say 'Actually, this isn't working. So next time we'll look at this, let's try and understand why it's not working.'" – P16

These community rules were expected to be enforced by **moderators**, but participants echoed each other to assert that an individual should not be permanently excluded from their community of peers, and the support and information they could receive:

> "There should be a little jail. They'll be allowed to come back, because you don't want someone to not be able to access the information." – P06

Explicit consent was mentioned as part of these community values, sustaining interactions between individuals:

> "So if you are talking on a one-to-one basis, because it's easier to ask the other person there to say 'I wanted to talk about this. Are you comfortable for me to talk about it?' They might say yes or no, so you have their consent." – P26

As expected, one of the most important rules was confidentiality, and we found our participants also expected any sharing activity to remain pertinent to the platform's purpose, and not descend into bullying, discrimination, or stray into irrelevant topics.
Participants stated that only **appropriate data** should be shared. Sharing data about sexual activity was mentioned numerous times as inappropriate, either because it might not be relevant or because it could offend individuals:

> "You know sometimes they can drift a bit into sexual practices, which perhaps is not appropriate but it can... it can get a bit ...a bit personal [...]" – P13

Not all those people who mentioned this were LGBQT, nor did all LGBQT participants mention this concern. Similarly, sharing certain data types was viewed with caution by participants, as these data might be ripe for abuse. For example, photographic images on the platform were sometimes seen as inappropriate because they could inadvertently disclose the HIV status of others in the photo, be offensive ("*No naked pictures... just thinking of all the bad things that could be going on down there!" – P06*), or might dilute the purpose of the data sharing platform (*"People just doing what they do on Facebook, like sharing pictures of their holiday." – P05).*
Another common theme centred on the dissemination of **correct information or medical advice**. This findings chimes with research in online communities, which has evidenced that users need to trust in the shared data being correct, and that trust is improved when moderation is put in place to remove incorrect or misleading information [27,42]. This particular concern was voiced in our interviews several times, as participants described instances where others promoted alternative medicine, e.g. garlic rubs, or outdated information, e.g. delaying starting ARVs. As P02 indicates, there was caution about sharing medical advice rather than opinion:

> "It's between you and your doctor to decide what medication you will take. [...] But I'm happy to exchange opinions about antidepressants, and why these antidepressants work for me, and why they don't work for me." – P02

4.3.5 Fostering the Sharing of Data. Considerations around how to foster responsible data sharing were raised by 24 participants. Sharing data was often conceptualised as an altruistic act, and an important part of community-building:

> "If it helps someone else, I'm sort of like, yeah, I don't mind helping you in your journey. And if you've got lots of questions I don't mind helping you out in that way." – P09

Overwhelmingly, our participants indicated that they would only be open to sharing their data with others if they **knew why** the individual wanted this information. They also expected **reciprocity in sharing**, for example, sharing similar data between individuals, and maintaining the balance between sharing and using that data, viewing sharing more like an exchange of assets. Research has highlighted the importance of **finding users who are similar to themselves** in attributes like age, date of diagnosis, and family status – seeing these similarities has previously been linked to building trust between users online [12,16,27,42,56]. Our participants' responses mirrored those findings, showing that an important consideration was to find smaller groups within the diverse HIV community. Some participants wanted to seek out particular groups to share data with on the platform, potentially based on gender, duration of diagnosis, and medication side effects. However, this should not be visible to the wider community:

> "Okay, like the trans community is one, and then you have the MSM community. And then you have like, the young people's community. And then you got like, people born with HIV… People finding out in one group that I was part of another group, that would kind of be outing myself to a wider community of people being able to see which communities I'm linked in with. Because like, people growing up with HIV, like, they only know me as one person, and if they suddenly saw me in the MSM group that would suddenly out me as gay, which I might be fine with but I feel like somebody else isn't going to be okay with it." – P07

Finally, whilst embracing the potential for sharing data to foster a sense of community, participants expressed **concerns about sharing data**. A worry was that individuals might be negatively impacted by self-comparisons with others, and indeed previous research has shown that users may avoid sharing data that might not be received positively by other members of the community, such as alcohol consumption in a weight-loss community [11]. For example, P11 did not want to share his lab results (CD4 and viral load) as he was not yet undetectable, an indicator of how well someone is managing their condition:

> "I'd deem it as a failure. […] I know some people physically cannot obtain the undetectable mark which is fair enough if you can't if you can't do it and you're trying your absolute best to do it." – P11

This is especially salient where not being undetectable on ARVs might be stigmatising due to the risk of onward transmission.

4.4 Summary of Results

Our findings cover three main points. First, we found that participants demonstrated active engagement with trust, privacy and security, and that their views on these were found to be strongly related to their own personal and digital identities and their relationships with other

entities (e.g. platform hosts, organisations, or community members). Participants used a variety of different reputation indicators to assess the trustworthiness of digital entities, such as well-known organisations in the community that might provide the platform. Access to a peer community was important but required some kind of 'gatekeeping' to ensure non-community members and untrusted entities were not admitted, with robust security measures akin to banking applications.

Second, while research focusing on cancer forums have found evidence that privacy was not in the forefront of users' minds when sharing health data [42], we found our participants to be highly sophisticated in their considerations of privacy. Privacy was seen to be achieved by making multifaceted choices over what data to disclose and share in a variety of settings with different entities, requiring privacy controls that allow specific data to be shared, managed and *retracted*. Our participants appreciated the benefits of sharing data with peers and they were, in broad terms, comfortable and willing to share personal, medical and lifestyle data via a digital platform with community peers. However, participants did not want to share data that could reveal their personal identity, such as name, email address or location, or details that they felt could lead to discrimination, such as sexual orientation.

Third, there was a strong sense of community-building in participants' considerations in relation to sharing data with peers. This may be particularly important among sub-groups within the HIV community, highlighting the importance of engaging with the intersectional experiences of those living with HIV. The community was viewed as built upon shared values emerging from 'grass roots' participation including confidentiality, explicit consent, rules that encourage people to feel a strong part of the community, and altruistic acts that serve a shared purpose. Similar to Huh et al.'s [27] findings for sharing of expertise and advice in online communities, sharing of data was seen as an exchange of data that was sometimes restricted to smaller sub-communities. In this respect, our findings also lay bare some tension between not wanting to share personal data because of the possibility of revealing their real identity with potential adverse consequences, and a recognition that personal details were needed to establish trust in digital identities and to find other sub-communities.

5 Discussion

This is the first study conducted in the UK to explore in detail how people living with HIV view trust, identity, privacy and security in the context of sharing their personal data with peers. Understanding their perceptions and concerns can, firstly, guide the development of trusted digital tools that will enable the secure sharing of their data with their peers, thereby providing support for people living with HIV and facilitating self-management of their health, and secondly, provide transferable insights on how to address such challenges for groups with other stigmatised long-term health conditions.

5.1 Design Implications For Building Peer Data Sharing Platforms Between People Living With HIV

Our work has shown that a platform hosted by, or endorsed by, a recognised HIV charity or medical organisation will enhance trust in the system. One approach is to co-brand a platform, including logos of supporting organisations, supported by clean, professional, and user-friendly interfaces to enhance a sense of trust [3]. However, our study also showed that perceived security within the trusted system is closely linked to a sense of personal safety in the context of people's social lives. In particular, the design of digital platforms needs to take into account how to make people feel safe in using it, for example through avoiding potential accidental disclosure of a user's HIV status through red ribbons or other imagery associated with the condition [6,7].

Strong privacy and security measures are key to fostering trust in such peer sharing platforms. Some data items were felt to be very sensitive as they could disclose their personal identity, and therefore should not be shared at all with peers; these included their name, email address and photo. Other data items – such as sexual activity or orientation – were felt to be inappropriate

or irrelevant to be shared, however this was governed by community rules of behaviour instead of privacy concerns. Most importantly, our participants conceptualised online privacy in terms of a consent model [51], whereby they wanted to give notice to opt in, or out, of sharing, or to withdraw access, and importantly to retain control of their decision making in the process. Significant for design is participants' multi-layered conceptualisation of privacy, and individuals' context-dependent decision-making about what to share and when. The platform would need to be flexible to accommodate what data an individual might want to share across time, and provide *contextual* control features that allow this to be carefully managed. The design and implementation of a platform for people living with HIV will also need to address the secure transmission of data, secure verification of their identity (e.g. through secure passwords and two-factor verification, as well as verification that they are indeed living with HIV). Many of our participants stated that, although potentially arduous, the most trustworthy means to verify users is to link security measures to existing medical processes, potentially through codes given out by clinics. The privacy and security measures put in place to protect users would need to be carefully explained and communicated, for example by a security policy document or visual security indicators (e.g. badges or certificates). Such propositions would require a non-trivial technical effort, and effortful steps on the part of the users. In considering this we are also mindful of critical accounts of online consent models; such models may be seen to create a false sense of security and transparency that is often not reflected in the actual system, either because of the challenge to implement, or because of the challenge to 'read' and understand associated privacy notices [51,60].

Therefore, a key design consideration is how to facilitate the sharing of data and sustained engagement with a system that is trusted, and not just trustworthy but actually secure. Our work has indicated that sharing data is best thought of as an exchange between individual community members, based around a common purpose, such as a question like how to better self-manage health – this is found to be motivating. However, further research is required to understand how to support this kind of exchange of data through a robust digital platform.

5.2 Data Sharing In Other Communities

Our study approaches hold two important lessons for researchers investigating other health communities. First, we make a methodological contribution to CSCW with our approach to investigating TIPS concerns with health communities. We worked closely with a peer researcher in a community organisation to design and conduct the study, and to develop our analysis and findings; thus, we are strongly informed by the community we engaged with. This way of working could be used as a model for future collaborations with health communities. Additionally, our mixed-methods study yielded rich insights from the analysis of both qualitative and quantitative data; and we encourage others to consider using privacy rating activities coupled with interviews to report on the TIPS concerns of communities in a way that retains the voices of individual participants.

Second, we believe that some of our findings with respect to trust, identity, privacy and security

could also extend to other communities that live with stigmatised health conditions, such as other sexually transmitted infections and mental health conditions. It makes sense that other communities might be equally sensitive to privacy and security concerns, and therefore might value the same privacy and security measures put in place to sustain responsible data sharing. However, there might be important differences in how these communities operate, which may influence the sharing of data. Whilst there is still much research to be conducted into the TIPS concerns of other communities, our work is a first step in shaping HCI and CSCW discourses in this area.

5.3 Limitations and Future Work

Our study was based in the UK, and only included English-speaking individuals who were interested in sharing data online. While we sought out a diverse group within the community of people living with HIV, we have not explored TIPS concerns and potential barriers to sharing data where culture, digital systems and medical processes might be markedly different. Investigating these concerns in other countries and/or other populations would provide important comparison points and additional knowledge in this area.

Our findings are based on hypothetical data sharing situations, and were often drawn from participants' informal sharing of data online through forums, or face-to-face in support groups. We are currently in the process of co-designing a digital platform to enable data sharing between people living with HIV, as well as investigating how this platform could be used as part of clinical consultations and research. We look forward to sharing the results of our design endeavours, as well as evaluations of its use in due course.

Finally, there are many more health communities that could benefit from data sharing but have not yet had the attention that they deserve. Our project is also investigating how TIPS concerns manifest in the context of mental health, and comparing these to the concerns of people living with HIV.

6 Conclusion

There is an increasing emphasis on supporting people living with HIV to self-manage their long-term condition through digital tools which support sharing of data. Our work reveals the TIPS considerations take need to be taken into account when building collaborative digital technologies for people living with HIV to share personal data with peers. In our interviews, we found that:

- Privacy and security played an important role in ensuring trust, relying on informed consent. Participants wanted to make fine-grained *choices* over what data was released to whom, for how long, and for what purpose. Tight security measures, akin to banking apps, were called for alongside verification of user identities. Decisions on sharing were often context-dependent.
- Participants were willing to share a variety of digital identity attributes, including personal, medical and lifestyle data, but not ones that would risk revealing their personal identity.
- Rules were expected to be put in place to ensure community-building and to foster sharing of data. The exchange of data was seen as an altruistic yet reciprocal act that respects appropriate community behaviour.

These insights can inspire other CSCW researchers who wish to facilitate data sharing in other peer health communities. We contribute key considerations and recommendations to inform the designs of trusted platforms that are sensitive to the TIPS concerns of people living with HIV. These technologies have a vital part to play in helping people to manage their condition and live well with HIV.

ACKNOWLEDGMENTS

We thank all our participants for sharing their time and experiences. This work was supported by the EPSRC (EP/R033900/1) .

REFERENCES

1. France Belanger, Janine S. Hiller, and A. J. Smith. 2002. Trustworthiness in electronic commerce: the role of privacy, security, and site attributes. *The Journal of Strategic Information Systems*: 245–270.
2. Virginia Braun and Victoria Clarke. 2006. Using thematic analysis in psychology. *Qualitative Research in Psychology* 3, 2: 77–101. https://doi.org/10.1191/1478088706qp063oa
3. Pam Briggs, Claire Hardy, Peter R. Harris, and Elizabeth Sillence. 2014. Patient-led perspectives on ehealth: how might hyperpersonal data inform design? In *Proceedings of HCI Korea* (HCIK '15), 115–121.
4. Carolyn Brodie, Clare-Marie Karat, John Karat, and Jinjuan Feng. 2005. Usable security and privacy: a case study of developing privacy management tools. In *Proceedings of the 2005 symposium on Usable privacy and security* (SOUPS '05), 35–43. https://doi.org/10.1145/1073001.1073005
5. Darren Brown, Shermaine Waugh, Adrian Bussone, and Simone Stumpf. 2017. Evaluation of BeYou+ an mHealth application to support self-management strategies for people living with HIV. Retrieved September 17, 2019 from https://onlinelibrary.wiley.com/doi/10.1111/hiv.12513
6. Adrian Bussone, Simone Stumpf, and Jon Bird. 2016. Disclose-It-Yourself: Security and Privacy for People Living with HIV. In *CHI 2016 Wporkshop on DIY Health.*
7. Adrian Bussone, Simone Stumpf, and George Buchanan. 2016. It Feels Like I'M Managing Myself: HIV+ People Tracking Their Personal Health Information. In *Proceedings of the 9th Nordic Conference on Human-Computer Interaction* (NordiCHI '16), 55:1–55:10. https://doi.org/10.1145/2971485.2971542
8. Adrian Bussone, Simone Stumpf, and Stephanie Wilson. 2017. The use of online forums by people living with HIV for help in understanding personal health information. *International Journal of Medical Informatics* 108: 64–70. https://doi.org/10.1016/j.ijmedinf.2017.10.001
9. Adrian Bussone, Simone Stumpf, and Stephanie Wilson. 2019. Designing for Reflection on Shared HIV Health Information. In *Proceedings of the 13th Biannual Conference of the Italian SIGCHI Chapter: Designing the Next Interaction* (CHItaly '19), 3:1–3:10. https://doi.org/10.1145/3351995.3352036
10. Yunan Chen and Heng Xu. 2013. Privacy management in dynamic groups: understanding information privacy in medical practices. In *Proceedings of the 2013 conference on Computer supported cooperative work* (CSCW '13), 541–552. https://doi.org/10.1145/2441776.2441837
11. Chia-Fang Chung, Elena Agapie, Jessica Schroeder, Sonali Mishra, James Fogarty, and Sean A. Munson. 2017. When Personal Tracking Becomes Social: Examining the Use of Instagram for Healthy Eating. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (CHI '17), 1674–1687. https://doi.org/10.1145/3025453.3025747
12. Andrea Civan-Hartzler, David W. McDonald, Chris Powell, Meredith M. Skeels, Marlee Mukai, and Wanda Pratt. 2010. Bringing the field into focus: user-centered design of a patient expertise locator. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (CHI '10), 1675–1684. https://doi.org/10.1145/1753326.1753577
13. Mayara Costa Figueiredo, Clara Caldeira, Tera L. Reynolds, Sean Victory, Kai Zheng, and Yunan Chen. 2017. Self-Tracking for Fertility Care: Collaborative Support for a Highly Personalized Problem. *Proceedings of the ACM on Human-Computer Interaction* 1, CSCW: 36:1–36:21. https://doi.org/10.1145/3134671
14. Jana Daher, Rohit Vijh, Blake Linthwaite, Sailly Dave, John Kim, Keertan Dheda, Trevor Peter, and Nitika Pant Pai. 2017. Do digital innovations for HIV and sexually transmitted infections work? Results from a systematic review (1996-2017). *BMJ Open* 7, 11: e017604. https://doi.org/10.1136/bmjopen-2017-017604
15. Tewfiq El Maliki and Jean-Marc Seigneur. 2013. Online Identity and User Management Services. In *Computer and Information Security Handbook (Second Edition)*, John R. Vacca (ed.). Morgan Kaufmann, Boston, 459–484. https://doi.org/10.1016/B978-0-12-394397-2.00025-8
16. Jordan Eschler and Wanda Pratt. 2017. "I'm so glad I met you": Designing Dynamic Collaborative Support for Young Adult Cancer Survivors. In *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing* (CSCW '17), 1763–1774. https://doi.org/10.1145/2998181.2998326

17. Susannah Fox and Maeve Duggan. 2013. *Tracking for Health.* Pew Research Center's Internet & American Life Project. Retrieved from https://www.pewresearch.org/internet/2013/01/28/tracking-for-health/
18. Jeana H. Frost and Michael P. Massagli. 2008. Social uses of personal health information within PatientsLikeMe, an online patient community: what can happen when patients have access to one another's data. *Journal of Medical Internet Research* 10, 3: e15. https://doi.org/10.2196/jmir.1053
19. Jeana Frost, Ivar E. Vermeulen, and Nienke Beekers. 2014. Anonymity versus privacy: selective information sharing in online cancer communities. *Journal of Medical Internet Research* 16, 5: e126. https://doi.org/10.2196/jmir.2684
20. Mads Frost, Afsaneh Doryab, Maria Faurholt-Jepsen, Lars Vedel Kessing, and Jakob E. Bardram. 2013. Supporting disease insight through data analysis: refinements of the monarca self-assessment system. In *Proceedings of the 2013 ACM international joint conference on Pervasive and ubiquitous computing* (UbiComp '13), 133–142. https://doi.org/10.1145/2493432.2493507
21. Allen L. Gifford and Erik J. Groessl. 2002. Chronic disease self-management and adherence to HIV medications. *Journal of Acquired Immune Deficiency Syndromes (1999)* 31 Suppl 3: S163-166. https://doi.org/10.1097/00126334-200212153-00016
22. Peter Gordon, Eli Camhi, Ron Hesse, Michelle Odlum, Rebecca Schnall, Martha Rodriguez, Esmerlin Valdez, and Suzanne Bakken. 2012. Processes and Outcomes of Developing a Continuity of Care Document for Use as a Personal Health Record by People Living with HIV/AIDS in New York City. *International journal of medical informatics* 81, 10: e63–e73. https://doi.org/10.1016/j.ijmedinf.2012.06.004
23. Andrea Grimes, Brian M. Landry, and Rebecca E. Grinter. 2010. Characteristics of shared health reflections in a local community. In *Proceedings of the 2010 ACM conference on Computer supported cooperative work* (CSCW '10), 435–444. https://doi.org/10.1145/1718918.1718992
24. Erik Grönvall and Nervo Verdezoto. 2013. Understanding challenges and opportunities of preventive blood pressure self-monitoring at home. In *Proceedings of the 31st European Conference on Cognitive Ergonomics* (ECCE '13), 1–10. https://doi.org/10.1145/2501907.2501962
25. Michael A. Hogg, Deborah J. Terry, and Katherine M. White. 1995. A Tale of Two Theories: A Critical Comparison of Identity Theory with Social Identity Theory. *Social Psychology Quarterly* 58, 4: 255–269. https://doi.org/10.2307/2787127
26. Jeffrey T. Huber and J. Michael Cruz. 2000. Information Needs and Information-Seeking Behaviors of HIV Positive Men and Women. *Medical Reference Services Quarterly* 19, 3: 39–48. https://doi.org/10.1300/J115v19n03_03
27. Jina Huh. 2015. Clinical Questions in Online Health Communities: The Case of "See your doctor" Threads. In *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing* (CSCW '15), 1488–1499. https://doi.org/10.1145/2675133.2675259
28. Jina Huh, Andrea Hartzler, Sean Munson, Nick Anderson, Kelly Edwards, John L. Gore, David McDonald, Jim O'Leary, Andrea Parker, Derek Streat, Meliha Yetisgen-Yildiz, Mark S. Ackerman, and Wanda Pratt. 2012. Brainstorming design for health: helping patients utilize patient-generated information on the web. In *Proceedings of the ACM 2012 conference on Computer Supported Cooperative Work Companion* (CSCW '12), 11–12. https://doi.org/10.1145/2141512.2141519
29. K. O. Hwang, A. J. Ottenbacher, A. P. Green, M. R. Cannon-Diehl, O. Richardson, E. V. Bernstam, and E. J. Thomas. 2010. Social support in an Internet weight loss community. *International Journal of Medical Informatics* 79, 1: 5–13.
30. Francisco Ibáñez-Carrasco, James R. Watson, and James Tavares. 2019. Supporting peer researchers: recommendations from our lived experience/expertise in community-based research in Canada. *Harm Reduction Journal* 16, 1: 55. https://doi.org/10.1186/s12954-019-0322-6
31. Maia Jacobs, James Clawson, and Elizabeth D. Mynatt. 2014. Cancer navigation: opportunities and challenges for facilitating the breast cancer journey. In *Proceedings of the 17th ACM conference on Computer supported cooperative work & social computing* (CSCW '14), 1467–1478. https://doi.org/10.1145/2531602.2531645
32. Maia Jacobs, Jeremy Johnson, and Elizabeth D. Mynatt. 2018. MyPath: Investigating Breast Cancer Patients' Use of Personalized Health Information. Retrieved April 24, 2020 from https://doi.org/10.1145/3274347
33. Maia L. Jacobs, James Clawson, and Elizabeth D. Mynatt. 2014. My journey compass: a preliminary investigation of a mobile tool for cancer patients. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (CHI '14), 663–672. https://doi.org/10.1145/2556288.2557194
34. James S. Kahn, Joan F. Hilton, T. Van Nunnery, Skip Leasure, Kelly M. Bryant, C. Bradley Hare, and David H. Thom. 2010. Personal health records in a public hospital: experience at the HIV/AIDS clinic at San Francisco General Hospital. *Journal of the American Medical Informatics Association: JAMIA* 17, 2: 224–228. https://doi.org/10.1136/jamia.2009.000315
35. Hyang-Sook Kim and S. Shyam Sundar. 2011. Using interface cues in online health community boards to change impressions and encourage user contribution. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (CHI '11), 599–608. https://doi.org/10.1145/1978942.1979028
36. Young-Ho Kim, Jae Ho Jeon, Bongshin Lee, Eun Kyoung Choe, and Jinwook Seo. 2017. OmniTrack: A Flexible Self-Tracking Approach Leveraging Semi-Automated Tracking. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 1, 3: 67:1–67:28. https://doi.org/10.1145/3130930
37. P. Kirwan, S. Croxford, M. Kall, K. Nambiar, S. Nash, M. Ross, L. Webb, H. Weeks, A. Wolton, and V. Delpech. 2019. Clinical outcomes and experiences of trans people accessing HIV care in England. In *HIV MEDICINE*, 11–11.
38. Tsai-Ya Lai. 2007. Iterative refinement of a tailored system for self-care management of depressive symptoms in people living with HIV/AIDS through heuristic evaluation and end user testing. *International Journal of Medical Informatics* 76: S317–S324. https://doi.org/10.1016/j.ijmedinf.2007.05.007

39. Yongbum Lee, Mieko Uchiyama, Kiyoko Kazama, Yasuko Minagawa, and Masaki Tsurumaki. 2015. Quantification of the Pain and Physical Burden Experienced during Positioning for Craniocaudal Imaging in Mammography, Evaluated by Measurement of Muscle Activity. *Health* 7, 1: 720–726. https://doi.org/10.4236/health.2015.71004
40. Ian Li, Anind Dey, and Jodi Forlizzi. 2010. A stage-based model of personal informatics systems. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (CHI '10), 557–566. https://doi.org/10.1145/1753326.1753409
41. Jingquan Li. 2013. Privacy policies for health social networking sites. *Journal of the American Medical Informatics Association* 20, 4: 704–707. https://doi.org/10.1136/amiajnl-2012-001500
42. Melanie Lovatt, Peter A. Bath, and Julie Ellis. 2017. Development of Trust in an Online Breast Cancer Forum: A Qualitative Study. *Journal of Medical Internet Research* 19, 5: e175. https://doi.org/10.2196/jmir.7471
43. Amneris E. Luque, Adjuah van Keken, Paul Winters, Michael C. Keefer, Mechelle Sanders, and Kevin Fiscella. 2013. Barriers and Facilitators of Online Patient Portals to Personal Health Records Among Persons Living With HIV: Formative Research. *JMIR research protocols* 2, 1: e8. https://doi.org/10.2196/resprot.2302
44. Haley MacLeod, Kim Oakes, Danika Geisler, Kay Connelly, and Katie Siek. 2015. Rare World: Towards Technology for Rare Diseases. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (CHI '15), 1145–1154. https://doi.org/10.1145/2702123.2702494
45. Lena Mamykina, Arlene M. Smaldone, and Suzanne R. Bakken. 2015. Adopting the Sensemaking Perspective for Chronic Disease Self-Management. *Journal of biomedical informatics* 56: 406–417. https://doi.org/10.1016/j.jbi.2015.06.006
46. Benjamin Marent, Flis Henwood, Mary Darking, and EmERGE Consortium. 2018. Development of an mHealth platform for HIV Care: Gathering User Perspectives Through Co-Design Workshops and Interviews. *JMIR mHealth and uHealth* 6, 10: e184. https://doi.org/10.2196/mhealth.9856
47. Phoenix K. H. Mo and Neil S. Coulson. 2008. Exploring the communication of social support within virtual communities: a content analysis of messages posted to an online HIV/AIDS support group. *Cyberpsychology & Behavior: The Impact of the Internet, Multimedia and Virtual Reality on Behavior and Society* 11, 3: 371–374. https://doi.org/10.1089/cpb.2007.0118
48. Phoenix K. H. Mo and Neil S. Coulson. 2014. Are online support groups always beneficial? A qualitative exploration of the empowering and disempowering processes of participation within HIV/AIDS-related online support groups. *International Journal of Nursing Studies* 51, 7: 983–993. https://doi.org/10.1016/j.ijnurstu.2013.11.006
49. Siti Hajar Mohd Roffeei, Noorhidawati Abdullah, and Siti Khairatul Razifah Basar. 2015. Seeking social support on Facebook for children with Autism Spectrum Disorders (ASDs). *International Journal of Medical Informatics* 84, 5: 375–385. https://doi.org/10.1016/j.ijmedinf.2015.01.015
50. Drashko Nakikj and Lena Mamykina. 2017. A Park or A Highway: Overcoming Tensions in Designing for Socio-emotional and Informational Needs in Online Health Communities. In *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing* (CSCW '17), 1304–1319. https://doi.org/10.1145/2998181.2998339
51. Helen Nissenbaum. 2011. A Contextual Approach to Privacy Online. *Daedalus* 140, 4: 32–48. https://doi.org/10.1162/DAED_a_00113
52. Francisco Nunes and Geraldine Fitzpatrick. 2015. Self-Care Technologies and Collaboration. *International Journal of Human–Computer Interaction* 31, 12: 869–881. https://doi.org/10.1080/10447318.2015.1067498
53. Aisling A. O'Kane, Helena M. Mentis, and Eno Thereska. 2013. Non-static nature of patient consent: shifting privacy perspectives in health information sharing. In *Proceedings of the 2013 conference on Computer supported cooperative work* (CSCW '13), 553–562. https://doi.org/10.1145/2441776.2441838
54. Aisling Ann O'Kane, Sun Young Park, Helena Mentis, Ann Blandford, and Yunan Chen. 2016. Turning to Peers: Integrating Understanding of the Self, the Condition, and Others' Experiences in Making Sense of Complex Chronic Conditions. *Computer Supported Cooperative Work (CSCW)* 25, 6: 477–501. https://doi.org/10.1007/s10606-016-9260-y
55. Aisling Ann O'Kane, Yvonne Rogers, and Ann E. Blandford. 2015. Concealing or Revealing Mobile Medical Devices?: Designing for Onstage and Offstage Presentation. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (CHI '15), 1689–1698. https://doi.org/10.1145/2702123.2702453

56. Kathleen O'Leary, Arpita Bhattacharya, Sean A. Munson, Jacob O. Wobbrock, and Wanda Pratt. 2017. Design Opportunities for Mental Health Peer Support Technologies. In *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing* (CSCW '17), 1470–1484. https://doi.org/10.1145/2998181.2998349
57. Tom Owen, Jennifer Pearson, Harold Thimbleby, and George Buchanan. 2015. ConCap: Designing to Empower Individual Reflection on Chronic Conditions using Mobile Apps. In *Proceedings of the 17th International Conference on Human-Computer Interaction with Mobile Devices and Services* (MobileHCI '15), 105–114. https://doi.org/10.1145/2785830.2785881
58. Siani Pearson. 2013. Privacy, Security and Trust in Cloud Computing. In *Privacy and Security for Cloud Computing*, Siani Pearson and George Yee (eds.). Springer London, London, 3–42. https://doi.org/10.1007/978-1-4471-4189-1_1
59. Jennifer A. Pellowski and Seth C. Kalichman. 2012. Recent Advances (2011-2012) in Technology-Delivered Interventions for People Living with HIV. *Current HIV/AIDS reports* 9, 4: 326–334. https://doi.org/10.1007/s11904-012-0133-9
60. Soo Young Rieh. 2009. Credibility and Cognitive Authority of Information. *Encyclopedia of Library and Information Sciences*, 1337–1344. https://doi.org/10.1081/E-ELIS3-120044103
61. Sabirat Rubya and Svetlana Yarosh. 2017. Interpretations of Online Anonymity in Alcoholics Anonymous and Narcotics Anonymous. *Proceedings of the ACM on Human-Computer Interaction* 1, CSCW: 91:1–91:22. https://doi.org/10.1145/3134726
62. Gabrielle M. Salib, Juan Fernando Maestre, Kenneth B. Nimley, Nadia Dowshen, and Gabriela Marcu. 2018. The Role of Reflection and Context in Medication Adherence Tracking for People Living with HIV. In *Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems* (CHI EA '18), 1–6. https://doi.org/10.1145/3170427.3188631
63. Aneesha Singh, Jo Gibbs, and Ann Blandford. 2019. Emotion and Experience in Negotiating HIV-Related Digital Resources: "It's not just a runny nose!" In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (CHI '19), 1–14. https://doi.org/10.1145/3290605.3300829
64. Shema Tariq, Valerie Delpech, and Jane Anderson. 2016. The impact of the menopause transition on the health and wellbeing of women living with HIV: A narrative review. *Maturitas* 88: 76–83. https://doi.org/10.1016/j.maturitas.2016.03.015
65. Ari Ezra Waldman. 2018. *Privacy as trust: information privacy for an information age*. Cambridge University Press.
66. Mark Warner, Juan F. Maestre, Jo Gibbs, Chia-Fang Chung, and Ann Blandford. 2019. Signal Appropriation of Explicit HIV Status Disclosure Fields in Sex-Social Apps used by Gay and Bisexual Men. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (CHI '19), 1–15. https://doi.org/10.1145/3290605.3300922
67. Elissa R. Weitzman, Emily Cole, Liljana Kaci, and Kenneth D. Mandl. 2011. Social but safe? Quality and safety of diabetes-related online social networks. *Journal of the American Medical Informatics Association: JAMIA* 18, 3: 292–297. https://doi.org/10.1136/jamia.2010.009712
68. Alan F. Westin. 1968. Privacy and freedom. *Washington and Lee Law Review* 25, 1: 166.
69. Paul Wicks, Michael Massagli, Jeana Frost, Catherine Brownstein, Sally Okun, Timothy Vaughan, Richard Bradley, and James Heywood. 2010. Sharing Health Data for Better Outcomes on PatientsLikeMe. *Journal of Medical Internet Research* 12, 2: e19. https://doi.org/10.2196/jmir.1549
70. Jing Zhang. 2017. Supporting Information Needs of Transitional Phases in Diabetes Management Through Online Health Communities. In *Companion of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing* (CSCW '17 Companion), 107–111. https://doi.org/10.1145/3022198.3024942
71. HIV/AIDS. Retrieved June 1, 2020 from https://www.who.int/news-room/fact-sheets/detail/hiv-aids
72. myHIV forum | Terrence Higgins Trust. Retrieved June 1, 2020 from https://www.tht.org.uk/our-services/online-services/myhiv-forum

A.1 Participant Demographics

ID#	Gender	Sexual Orientation	Age	Ethnicity
P01	Man (cis)	Homosexual	46	White British
P02	Man (cis)	Homosexual	53	White Other
P03	Man (cis)	Homosexual	31	White British
P04	Man (cis)	Homosexual	53	White British
P05	Man (cis)	Homosexual	33	Latin
P06	Woman (cis)	Heterosexual	40	Black British Caribbean
P07	Man (trans)	Queer	20	White British
P08	Woman (cis)	Heterosexual	59	White British
P09	Woman (cis)	Heterosexual	25	Black British Caribbean
P10	Man (cis)	Heterosexual	45	Black British African
P11	Man (cis)	Heterosexual	26	Black British African
P12	Man (cis)	Homosexual	57	Mixed White and Black African
P13	Man (cis)	Homosexual	63	White British
P14	Woman (cis)	Heterosexual	49	White British
P15	Woman (cis)	Heterosexual	63	Black British African
P16	Woman (cis)	Heterosexual	20	Black British African
P17	Woman (trans)	Heterosexual	43	White Irish
P18	Man (cis)	Heterosexual	26	Black British African
P19	Woman (cis)	Heterosexual	58	Black British African
P20	Man (cis)	Heterosexual	41	Asian British
P21	Woman (cis)	Heterosexual	54	Black British African
P22	Woman (cis)	Heterosexual	39	Black British African
P23	Man (cis)	Bisexual	54	White British

P24	Woman (cis)	Heterosexual	47	White Other
P25	Man (cis)	Heterosexual	54	Black British African
P26	Man (cis)	Heterosexual	52	Black British African

A.2 Coding Schemes

Coding Scheme 1: Trust, Privacy and Security Understanding codes

Aspect	Code	Definition	Sub-Code	Definition	Participant Count
Trust	Trustee	The identity that is being trusted to do or not do something (not the context in which things are trusted e.g. 'I trust people online' where people are the trustee, not online)	Unspecified	Unspecified other identities *'People', 'Someone', 'Others', 'users'*	14
			Professionals	Individuals working in a professional capacity (not necessarily limited to healthcare workers) 'my health team' 'medical professionals', 'my doctors', 'a professional'	4
			Organizations	A professional organization (formalized group of people), e.g. NHS, sexual health charity, THT, NAM, or unspecified 'organizations'	4
			Digital Systems	A digital system or technology which the participant has placed trust in / not placed trust in. *'A website,' 'The system', 'the platform'* Not instances where digital systems are provided as the context for trust	5
	Expectation	What the trustee is expected to do	Best interest	Statements about trusting others to	14

		or not do (the behaviour the trustee is trusted to carry out)		act with the participant's best interest in mind, to do the right thing for the participant, and to act as agreed upon	
			Confidentiality	Statements about trusting others to keep something confidential, not pass it on, not share it with others, and handle it with care	15
	Not a Definition of Trust	Any statement which does not include both a Trustee and an Expectation	N/A	N/A	2
Privacy	Choice	Statements indicating that there may be some data that is not always wanted to share, or that may be preferred to keep hidden. Can include specific examples of choosing who to share/not share with, or even where the choice is not given.	N/A	N/A	15
	Data	Statements indicating that data/information	N/A	N/A	17

		should be shared / should not be shared. May be specific (e.g. 'making out with someone') or general ('something') or even insinuated ('I don't want to give that out')			
	Domain	Statements about the domain in which privacy is desired / takes place. Could be a location (e.g. online, in the club, in public) or a scenario (e.g. dating, a conversation between two people,	N/A	N/A	9
	Not a definition of privacy	Statements which do not include Choice AND Data codes	N/A	N/A	8
Security	Protection	Statement indicating the safety of something, protection of something, a mechanism for protecting something, etc. *'__ is protected', 'under lock and key', 'kept from trolls'*	N/A	N/A	16
	Protected object	Statement indicating a THING (data, identity, person, even 'it' or 'something') is protected.	Data	Data related to health, HIV, personal details, or other unspecified information	17
			The Individual	Reference to a person, such as the participant, being protected and kept safe.	4

	Not a definition of security	Statements which do not include Safety AND Object codes	N/A	N/A	5

Coding Scheme 2: TIPS considerations codes

Theme	**Definition**	**Sub-theme**	**Definition**	**Participant Count**
Security Features	References to having security features in place, or referencing specific security features to include. E.g. passwords, firewalls, auto log-out, etc.	Log-In Security	Mention of security features for logging in (e.g. passwords, thumb print, auto-log out, lock out after three attempts)	13
		Data Security	Mention of security features to keep data secure. Could be generic ('have the best security possible to protect my data!') or specific ('firewalls') etc. ALSO include comments about expecting or wanting to see statements describing the implemented security features	13
		Verification	Comments about sign-up process, method of verifying who they say they are / that they are HIV+, or ways of keeping out those it is not meant for	18
Privacy Features	Statements about ways of maintaining privacy, desired privacy features, privacy policy, etc.	Identifiability	Statements about whether the participant would add/track/share data that was identifiable to them, or thoughts on whether users should be identifiable or anonymous. E.g. "I definitely wouldn't use my real name" "It should keep people from sharing their last name"	17
		Privacy Policy	Comments about looking for, wanting, needing, etc. a	7

			statement that outlines the privacy policy	
		Privacy controls	Interface elements/features allowing users control over what is shared (WHAT is shared goes under identifiability). Also includes desire for reminders/warnings when sharing	12
		Obvious HIV indicators	Comments about the impact of having a red ribbon, reference to HIV, or other obvious link to HIV as a visual for the platform	16
Rules of Interacting	Comments about wanting/expecting something outlining appropriate and inappropriate ways of interacting. Rules of Engagement. Also includes comments about having admins or moderators in place, reporting, banning, blocking features	N/A	N/A	23
Sharing Behaviour	Comments about considerations for sharing data BEYOND identifiable concerns. Reasons for sharing, reasons for not sharing, expected behaviours of others when sharing	N/A	N/A	24
Reputation Indicators	Facets that indicate the host / community / individual's reputation that can help to assess their credibility. Includes aspects around look and	N/A	N/A	22

	feel that indicate reputation, or how their behaviour or past behaviours/actions indicate their reputation			

APTENDOFDOCAPT
APTENDOFDOCAPT