Disclose-It-Yourself: Security and Privacy for People Living with HIV

Adrian Bussone, Simone Stumpf and Jon Bird
Centre for Human Computer Interaction Design
School of Mathematics, Computer Science and Engineering
City University London
London, UK, EC1V 0HB
Adrian.Bussone.1@city.ac.uk

Abstract
There are increasing numbers of people living with chronic diseases who track, reflect upon and even share their personal health data. However, attention to the privacy and security needs of stigmatised chronically-ill users has been scarce. We present the early results of ten interviews with people living with HIV about their Personal Health Informatics requirements. We found that they require strong security measures whilst privacy settings need to be highly configurable to meet their needs, which vary over time and by context. Our findings indicate that ‘Do It Yourself’ control over how their health information is disclosed and accessed is key for these users to trust a system. Current personal health informatics technology does not meet the needs of most of the participants and the majority use paper-based tracking systems, such as diaries.

Author Keywords
Personal Health Informatics; Privacy; Security; People Living With HIV

ACM Classification Keywords
H.5.m. Information interfaces and presentation (e.g., HCI): Miscellaneous

Introduction
Personal informatics considers the technology and information needs of individuals who collect data about themselves and reflect on, and potentially share, those data to draw out a deeper understanding of their behavior [4]. The most common reason to track data is related to health [4], and this has given rise to Personal
Health Informatics (PHI). The use of PHI technology is encouraged in the healthcare industry [2], and the literature has shown examples of chronically ill end-users drawing valuable insights related to their health [5,8,14]. This paper presents work on the appropriation of existing PHI technologies, and privacy and security practices as aspects of DIY behaviour.

Nearly half of American adults are living with a chronic disease [7] (e.g. diabetes, COPD, and HIV [16]). Each disease is associated with a different level of stigma – and for some conditions societal opinions can be extremely harsh. Research on medical device use suggests that stigma actually influences the needs and behaviour of users [13]. We can therefore expect that the level of stigma associated with different chronic diseases will result in different user needs. While research has begun to focus on supporting users in tracking their personal health information (e.g. [5,10,13]), little work [1,9,12] has focused on the privacy and security needs of stigmatized groups like HIV (an under-researched group with regards to HCI).

We conducted a qualitative study aimed at understanding the PHI needs of people living with HIV (PLWH). This study focused on the DIY practices of these individuals, not on access control for healthcare workers. HIV is a highly stigmatized chronic disease and PLWH would benefit from technology that supports their tracking needs [15] or sharing processes [11].

Our early findings suggest that the stigma around HIV results in a need that technology does not currently meet: control over the privacy and security of their personal health data. By sharing our findings, we hope to begin a discussion about how future PHI designs can support users’ DIY privacy and security needs.

**Study Design**

We conducted semi-structured interviews with PLWH in the UK who track their personal health data. We recruited ten individuals through sexual health organizations, social media, and online forums. Participants were asked to fill out a questionnaire aimed at gathering demographic details. Next, they were interviewed for approximately 30 minutes about how they track and use their personal health data and if their needs were currently met. Participants were interviewed in private locations in London or online over Skype, and were reimbursed for their travel costs, when appropriate.

The interviews were audio-recorded and transcribed in full. In order to ensure the confidentiality of each participant all identifiable data captured were anonymised. One coder analysed the transcripts using Grounded Theory [6]. Using a bottom-up process, it quickly emerged that our participants were very sensitive to the security and privacy of their health data. We focused on these aspects in more depth in our analysis, developing nine sub-codes. We now present the major themes that came out of the analysis related to privacy and security.

**The Necessity of Security**

By security we mean the safety of the user's personal information and how it is protected against unwanted access [3], whether for disclosure or abuse. All of our participants made statements showing that the security of their personal health information was very important to them.

Eight participants tracked their health information using a paper-based diary (Table 1), six of these said that it

<table>
<thead>
<tr>
<th>ID</th>
<th>Tracks with:</th>
<th>Encryption method:</th>
</tr>
</thead>
<tbody>
<tr>
<td>P01</td>
<td>Website</td>
<td>Vague language</td>
</tr>
<tr>
<td>P02</td>
<td>Paper diary</td>
<td>None</td>
</tr>
<tr>
<td>P03</td>
<td>Paper diary</td>
<td>None</td>
</tr>
<tr>
<td>P04</td>
<td>Paper diary</td>
<td>None</td>
</tr>
<tr>
<td>P05</td>
<td>Paper diary</td>
<td>Initials, foreign language</td>
</tr>
<tr>
<td>P06</td>
<td>Paper diary</td>
<td>Unique terminology</td>
</tr>
<tr>
<td>P07</td>
<td>Paper diary</td>
<td>None</td>
</tr>
<tr>
<td>P08</td>
<td>Paper diary</td>
<td>None</td>
</tr>
<tr>
<td>P09</td>
<td>Calendar</td>
<td>Tick marks</td>
</tr>
<tr>
<td>P10</td>
<td>Health app</td>
<td>Vague language</td>
</tr>
</tbody>
</table>

Table 1: Methods participants use to track and encrypt their personal health data
was because they were not confident in the security of
digital tools. Of the eight, all considered paper to offer
digitally, six of the eight responded favorably – with
the highest security, as they could keep it hidden: "A
caveat that the tool needed to demonstrate high levels
diary you can hide it, nobody can come in your room
of security: "Something that would be better? Well as
and take it." (P05) However, when asked if they would
of now I don’t have any option. I don’t have an option.
be interested in tracking their health information
Nothing is laid out for me to give me an option." (P06)
digitally, six of the eight responded favorably – with
There was no agreement over where data would be
the caveat that the tool needed to demonstrate high levels
stored, locally or in the cloud: "With all that’s
of security: "Something that would be better? Well as
happening with the bank details online, things like that,
the highest security
one thing I don’t do with my HIV [data], I don’t put it
of security: "Something that would be better? Well as
on the cloud. I don’t do that." (P02)
out the cloud. I don’t do that." (P06)
Two participants used digital PHI tools, and confidence
Sharing with HIV
in the security of their personal health data seemed to
P05
play an important role in the decision to use these. For
8 MD, HIV+
example, one of the two used a website linked to a
MD, HIV+, friends
well-known HIV organization (THT), which he later
8 MD, HIV+
explained as a decision made on trust: "I suppose I’ve
family
P06
got an element of trust more so in a company I know
11 MD, HIV+, friends
and trust, such as THT. … But if it was just an app
P07
made by a company with a snazzy name, I don’t know.
8 MD, HIV+
I wouldn’t have as much faith." (P01)
family
P08
<1 MD, HIV+
P09
12 MD, HIV+
P10
19 MD, HIV+, family

Table 2: Participants' time since diagnosis and information access control

In addition, to enhance security even more, three of
the eight participants using paper diaries also used
results: "I just have to use jumbled language, which no
some form of 'encryption' to avoid accidental disclosure
one would understand when they see it." (P06) This
of their information. For example, one participant
‘encryption’ also extended to the two participants using
tackled his medication compliance on a calendar with
digital tools. Both reported using vague terminology in
an subtle tick mark, while another wrote in a paper
the reminders they set for taking their medication: "I
the tools. Both
information online
without my
diary you can hide it, nobody can come in your room
just get a little text that says 'Remember that thing.' …
and take it." (P05) However, when asked if they would
might see this information, and can it be shared
You can get it specific if you want, but 'Remember that
be interested in tracking their health information
without my permission? HIV-specific websites and
forums were commonly felt to be safe places where information would only be seen by other PLWH. However, most participants still preferred to remain anonymous by using ambiguous screen names to mask their identity: "I mean, I like the forums on Reddit for HIV because it’s anonymous." (P08) Two participants did disclose their identities on HIV websites and forums because they felt their information was protected from HIV- individuals due to of the nature of the website: "I’m there on the website with my photo. I don’t really fear it. No one is going to see it unless you go there, unless you’re one of the members." (P05)

When sharing online in other places, such as Facebook, participants considered their lack of control over others accessing the information without their consent. The danger of this being that the information could be seen by people to whom they had not disclosed to. Indeed, every participant made statements suggesting this to be a major concern: "I use my picture if it is only open to me. If I want to share, I put a symbol. Yeah. I put a symbol if I want to share with my friend because I don’t know who has access to that information." (P02)

Participants also indicated that their privacy concerns changed over time as they become more comfortable with their diagnosis: "Um, at the beginning I wouldn’t put anything [on-line]. But um, I think, it depends. I’m at a point now where I don’t care about my status. … It’s there, it’s on Facebook." (P04)

Discussion
Our findings have three implications for the design of Do-It-Yourself PHI technology:

1. Assurance that personal health data is securely stored: There was interest in tracking digitally amongst those using paper but little consensus on what storage location was most secure. PHI technologies could be made more attractive by: a) enabling users to specify the storage location; and b) clearly communicating to users the security measures that are provided.

2. Enhanced security mechanisms: Our finding that users actively use a variety of methods to encrypt their data suggests the need for further research into how DIY encryption methods can be supported (in line with [1]).

3. Privacy-preserving access control: There was a willingness to share personal health information with people that have a professional need to know it (e.g. doctors) or are unlikely to abuse that information (e.g. other HIV+ users). However, users still need to be able to select what information can be accessed by others on an individual basis. Additionally, there should be control over how – or if – that data can be shared further and this might change over time. This indicates the need for highly customisable access policies that support the user’s 'locus of control' [9].

Our study is a first step in investigating how PLWH would like to track and share their health information. In order to increase adoption and continued use of PHI technology among stigmatized chronically-ill users, designers need to be sensitive to their DIY privacy and security needs.

Acknowledgements
We thank our participants for their time and sharing their experiences with us.
References
13. Aisling Ann O'Kane, Yvonne Rogers, and Ann E. Blandford. 2015. Concealing or Revealing Mobile

15. Rebecca Schnall, Suzanne Bakken, Marlene Rojas, Jasmine Travers, and Alex Carballo-Dieguez. 2015. mHealth Technology as a persuasive tool for treatment, care and management of Persons Living with HIV. AIDS and Behavior. 19, 2: 81-89.