Current HIV/AIDS Reports (2020) 17:180–189
https://doi.org/10.1007/s11904-020-00489-z

EHEALTH AND HIV (J SIMONI AND B GUTHRIE, SECTION EDITORS)

Ethical Considerations in HIV eHealth Intervention Research: Implications for Informational Risk in Recruitment, Data Maintenance, and Consent Procedures

Celia B. Fisher[1] · Elise Bragard[2] · Rachel Bloom[2]

Published online: 2 May 2020

Abstract

Purpose of Review Along with the benefits of eHealth HIV interventions are challenges to participant privacy and confidentiality inherent in the use of online strategies. This paper reviews current guidelines and recent publications to identify ethical issues and suggested solutions in recruitment, data management, and informed consent.

Recent Findings Across eHealth HIV research, recruitment, data collection, and storage efforts to protect informational risk highlight the tension between the investigators' ability to protect participant confidentiality and the evolving informational risk posed by the online platforms on which they are operating. Adequately addressing these challenges requires updating technical competencies and educating participants on their own responsibilities to guard against privacy violations. Additional protections are required when interventions involve peer or community support, especially with minors.

Summary The rapid progression of technology presents challenges in solidifying best practices for future interventions. This article draws on published works describing investigator experiences to contribute to the ongoing development of guidance in this area.

Keywords HIV · eHealth · Mobile research · Informed consent · Data privacy · Research ethics · Online recruitment

Introduction

With over 90% of US adults regularly using the internet, healthcare-related services are increasingly conducted online [1]. eHealth interventions, healthcare services delivered through electronic communication devices, carry the promises of lowering participant travel and related cost burdens, expanding access to services in underserved populations, and offering privacy and discretion when participants are asked to provide information related to socially sensitive information. People with or at-risk for HIV is in a position to derive significant benefit from this model of healthcare delivery, and eHealth interventions have increased the points of access for delivering HIV-related care. eHealth interventions have been developed to encourage antiretroviral therapy (ART) medication adherence, to expand accessibility to pre-exposure prophylaxis (PrEP), to refer participants for HIV testing, to strengthen connections with healthcare systems, to encourage less-risky sexual behavior, and to facilitate community building and improve participants' trust in intervention teams [2–5].

People at risk for or living with HIV indicate that privacy protections and maintaining confidentiality are key factors influencing their willingness to engage in eHealth intervention research [3, 6, 7]. As internet-based technology rapidly progresses, online users are often unaware that sensitive data can be shared without their permission, leading researchers to seek more up-to-date guidelines for safeguarding participant privacy in HIV-related eHealth modalities [8•]. While research organizations and governmental institutions have issued recommendations for conducting online research and recruitment, a consensus document on guidelines specific to HIV eHealth interventions and research has yet to emerge [9–12]. The Association of Internet Researchers (AoIR), the American

This article is part of the Topical Collection on *eHealth and HIV*

✉ Celia B. Fisher
fisher@fordham.edu

[1] Center for Ethics Education and Department of Psychology, Fordham University, 117 Dealy Hall, Rose Hill Campus, 441 E. Fordham Road, Bronx, NY 10458, USA

[2] Department of Psychology, Fordham University, Bronx, NY, USA

Psychological Association (APA), the Secretary's Advisory Committee on Human Research Protections (SACHRP), and the British Psychological Society all provide guidelines for conducting internet-enabled research that is not specific to HIV [10, 12–15]. The American Journal of Bioethics (AJOB) and the National Institutes of Health (NIH) have published guidelines on ethical online recruitment procedures using social media, but these do not extend into discussions on interventions [11, 16, 17]. The APA has also released guidelines for protecting privacy in telehealth interventions [18, 19], but these do not address issues specific to HIV (mobile health) mHealth methods. Many published articles on HIV-specific best practices with online research do not describe specific approaches to mitigating privacy challenges, and prior reviews have not been updated to reflect the issues raised by the current eHealth landscape [17, 20].

This paper outlines the ways in which HIV eHealth research teams can competently enhance participant trust by staying abreast of current challenges to privacy and confidentiality across online recruitment, data collection, and management, as well as implications for informed consent. We review previously published eHealth guidelines while integrating procedures and recommendations found in the method and discussion sections of current eHealth HIV research.

Methods

The authors conducted a literature search in September, 2019, for articles on eHealth HIV interventions through PubMed, PsycInfo, and Google Scholar databases. The initial search terminology included "HIV" and "eHealth" or "mHealth" or "electronic health" or "mobile health," as well as "HIV" and "intervention" and "online recruitment" or "online research" or "online." Reference lists and bibliographies served as sources for additional relevant articles that the literature search excluded.

Forty-five articles matched initial search criteria, which the authors analyzed and coded as follows: population (age range, sexual behavior, and HIV status), type of research (intervention, usability testing, and focus group), focus of the subset of intervention studies (HIV prevention versus HIV treatment maintenance), recruitment procedures (online or through clinics), technological implement (computer, user's existing mobile device, provided mobile device, or other electronic modality), privacy procedures (whether any were implemented and, if so, the actions taken by the research team), and scope (USA versus international). The authors included only peer-reviewed empirical articles HIV eHealth or mHealth prevention or intervention approaches.

Exclusion criteria included publication prior to 2014, primarily international research focus, and no concrete discussion of an HIV intervention. Additionally, articles that discussed online recruitment procedures but then exclusively reported on an offline (e.g., in-clinic) HIV intervention were excluded. Of the initial 45 articles, 24 research studies met eligibility criteria for inclusion in this review. With few exceptions, these articles were published subsequent to an extensive review article on internet-based interventions addressing the HIV care continuum published in *Current HIV/AIDS Reports* in 2015 [21].

Many empirical articles regarding eHealth interventions for HIV treatment and prevention did not adequately provide guidance or best practices on safeguarding participant privacy, in some cases not mentioning any confidentiality concerns. After the initial literature search, the authors conducted a secondary online search of eHealth and mHealth intervention guidelines and review articles that were not necessarily exclusive to HIV treatment and prevention in order to support knowledge-building around existing discussions on privacy protections in eHealth. The authors also reviewed online publications and other resources from government and scientific organizations using the search terms described above. The next sections of this article describe procedures and recommendations for data security practices in online recruitment, data maintenance, and informed consent.

Online Recruitment

Researchers face various ethical challenges when conducting online recruitment for eHealth studies with populations at elevated risk of HIV infection and people living with HIV (PLWH). In this section, we draw on guidelines for social media recruitment, recommendations for use of social media-targeted advertisements, and the ethical challenges investigators report facing when ensuring response validity during recruitment [11, 14, 16].

Social media sites and geosocial messaging or dating applications that allow targeted advertisements based on profile content and geographic location can be an effective and cost-efficient way of sampling a target population, allowing researchers to more effectively recruit diverse samples of "hidden populations" for HIV eHealth studies [22]. However, when a potential participant clicks on an ad for a research study, the host website automatically collects information about that person's interests and affiliations based on their profile, leaving an identifiable digital trail [16, 23]. As a consequence, depending upon the nature of the study and the specifics of the inclusion criteria, information regarding prospective participants' characteristics can be inferred and is available to the companies running these applications. Third parties collect this data before individuals have the chance to learn about potential privacy and confidentiality risks, and even if the individual decides to exit once landing on the recruitment site. A recent study indicated that men who have sex with men (MSM) responding to research ads on several popular sexual minority dating sites indicated greater trust in researchers collecting such data compared with social media companies, but were not aware that those sites could collect information simply from their engagement with the study advertisement [24•].

To maintain participant trust, researchers can strive to educate themselves about the Terms of Services for their recruitment sites to understand how involved companies are protecting and using participant data. In addition, they can host eligibility screener surveys on secure servers that are HIPAA compliant [25, 26]. An alternative, albeit more time-intensive, strategy is to recruit participants from social media or geosocial dating applications but only collect identifiable information offline by conducting in-person or phone eligibility screenings with participants [27].

Researchers can also recruit online through posting study announcements on community message boards or chatrooms, or by creating researcher profiles on geosocial dating applications and reaching out to other users with the purpose of study recruitment [28]. This form of recruitment raises user privacy concerns. For example, user profiles on community message boards or dating applications may contain real names, photos, and HIV status, and users may not expect this kind of information to be viewed by researchers. One study found that some members of these online communities felt that researchers who created user profiles for study recruitment were encroaching on spaces they valued as private and safe [8•]. This recruitment strategy is ethical as long as the profile makes it clear that the user is a research staff member, that messages are restricted to detailed research recruitment language, contact can only be made when app users initiate a chat with research staff, and that no other forms of communication between research staff and users are permitted [29]. Some social media sites now have updated their Terms of Service to block researchers from soliciting users to join studies, which further protects users from research teams violating ethical restrictions [30].

Challenges to Data Validity

Online recruitment provides the opportunity to cast a wider net for identifying potential subjects. However, it may also allow individuals to mislead researchers about their actual eligibility for the study [23]. Researchers recruiting participants for HIV eHealth studies therefore need to design data validation protocols to prevent inclusion of ineligible, repeat, or purposefully fraudulent participants. Automated bots are software applications designed to run online tasks, such as completing a survey, at a much higher rate than would be possible for a human. Since most online research studies offer compensation, automated bots have been developed to fraudulently enter large numbers of studies and secure the incentive. The promulgation of these bots has jeopardized the data integrity of online research, necessitating stringent data validity checks. Recommended automatic and manual protocols that can be used in online studies include cross-checking demographic information such as age and date of birth or state and zip code, comparing responses from similar email addresses (often raising suspicion because they will vary in one or 2 letters), checking for responses from identical IP addresses, and using timestamps to evaluate duration of the survey response (because rapid response times could indicate that automated bots are initiating fraudulent submissions) [31, 32]. Some researchers require participants to enter phone numbers or email addresses during eligibility screening in order to ensure data validity and prevent against fraudulent participants or automated bots [33].

Validation checks for recruitment can become more complicated for researchers wishing to conduct online research on serodiscordant couples. To help ensure validity, research teams must first validate individuals as eligible participants who can then provide an email address for their partner to be contacted by the research team [34]. Researchers must then validate the partner's identity and eligibility, and further verification around relationship length and shared interpersonal knowledge is required to ensure the participants are in a legitimate relationship [26]. Automated processes may flag discrepancies that do not warrant excluding the data, for example, two individuals might respond differently about the relationship length because there was a period of separation. The automated process may also flag repeat IP addresses as potentially fraudulent, but if a couple lives together they may use the same computer. For these reasons, it is a best practice to manually review the results of automated validity checks.

Online snowball sampling or respondent-driven sampling (RDS) allows researchers to sample hard-to-reach and diverse populations by engaging current participants in recruiting (e.g., forwarding the survey link) to eligible participants in their network [31]. This adds an additional level of privacy for those in the network and can help counteract research distrust since it avoids asking current participants to provide researchers with the email addresses of their friends or other contacts [35]. However, when snowball sampling or RDS is conducted solely online, it can pose challenges for data integrity, as existing participants may inform referred contacts about the eligibility criteria, enabling ineligible participants to modify their screener responses to gain study access. This requires investigators to both train and monitor the strategies of peer recruiters. For example, in one study utilizing peer-recruiters for an eHealth intervention conducted on a social chat room, in addition to training the recruiters, researchers used validity checks to make sure the new participants' affiliated social media accounts were authentic by ensuring the account was connected to the peer-leader and had more than 50 followers [36].

Data Maintenance Strategies

The participant data research teams collect during eHealth interventions may be stored in and transferred between multiple online locations. These include university servers, cloud-based back-up software, third-party survey or intervention platforms, social media sites, and mobile applications on participant devices. Several organizations, including the AoIR, the APA, the British Psychological Society, the NIH, and the SACHRP provide guidelines for appropriately de-identifying, storing, and transferring participant data to minimize data breaches and informational risk, with an emphasis on proper encryption and protocol for data destruction [10–12, 14, 15]. These guidelines offer strategies for restricting access to study data, authenticating participants and researchers, encrypting all data gathered online, and strongly recommend clearly describing safeguards for the collection, storage, processing, and destruction of participant data.

Published articles on eHealth HIV studies increasingly describe the use of secure servers for data storage, specifying whether their institution or third parties host them. Some authors also indicate when these servers are HIPAA-compliant [26, 37]. The use of HIPAA-compliant servers are required when studies involve participant authorization to access their administrative health records or when health-related data collected by the study will be included in a patient's health record. HIPAA criteria are also useful for guiding confidentiality protections even when data will only be used by investigators. HIPAA-compliant storage safeguards should prevent bad actors from illegally accessing or hacking health records transmitted through a network, which include rules about who can access records, prevent manipulation or destruction of health data, and have a system in place for auditing user activity [38].

When intervention or research teams use personal health information (PHI) from clinics or hospital systems, they need to be aware of which data feeds back into those electronic records and how to maintain HIPAA compliance in the process [39]. Training clinicians and research teams are therefore essential in protecting participant confidentiality and supporting the development of trust between participants and front-line staffs. Some have suggested that to keep pace with technological progression, eHealth intervention devices or applications used in a clinical setting need to be regulated in a similar process to medical devices [40].

In their journal articles, eHealth researchers seldom include reports of whether encryption was used for data transferal, and there is evidence that few eHealth applications use encryption [40]. When participant data from an app is uploaded from cellular or wireless networks to study servers for analysis, there is a risk of a security breach occurring during transmission. Ethical guidelines published by the Journal of Medical Internet Research recommend that mobile applications use encryption for the storage and transmission of data to prevent against hacking and identity theft [40]. Researchers also should be aware that government agencies and telecommunication companies can potentially access data transmitted through wireless networks and that telecommunication companies may claim ownership of such data. One data maintenance strategy used in eHealth HIV studies involves de-identifying subject data and coding with unique numbers immediately after collection so that identifiable data is not stored on any servers [41].

Another key privacy concern in eHealth HIV studies is the secure storage and handling of data contained in messages or posts written by participants on online discussion boards or chatrooms used or created by the study team. These posts may be accessible to individuals outside the group if a participant's name or username is entered into a search engine, and employers, admissions officers, and even prospective romantic partners commonly search for this type of information [42–44]. When researchers carry out interventions on social media sites or geosocial dating applications, they must also consider that these companies may also have access to and ownership of participant data [36]. Researchers must ensure they are knowledgeable about such companies' respective Terms of Services to assess whether there is a possibility they might sell participant data to third parties for marketing [23].

Researchers must also be aware of the privacy and confidentiality limits of any third-party software they use to analyze data. To protect participant data, investigators can use a third-party analytics app to extract group engagement data. These applications do not extract or store members' profile data, but only engagement data such as *likes* and comments [36]. Collaborating with third-party software developers also requires constant communication adjustment to ensure that the technology meets the research goals and ethical standards [45].

Efforts to ensure data security may also be restricted based on the compliance policies of researchers' home institutions. For example, the developers of one intervention originally designed on a popular social media site tried to move the intervention to a newly created platform after negative participant feedback [45]. The university compliance officer blocked them because it was not possible to store the new software on university secure servers. This example highlights the importance of working with institutional technology and compliance offices in the design of data security protections from a project's inception.

Use of Mobile Devices

HIV researchers assess mHealth interventions using SMS and mobile applications as promoting HIV testing, preventative behaviors, PrEP or ART adherence, and knowledge of PrEP [21, 31, 37, 46]. There are additional privacy risks for participants in mHealth interventions because of the ease by which mobile phone data can be accessed by third parties [13, 20, 40]. One mitigating strategy is the appropriate deletion of data when there is a risk of a security breach, and instituting protocol for remotely wiping participant data within intervention applications if the phone is lost [47]. Research teams can ask participants to use biometric identification such as thumbprints to access the intervention app and the sensitive personal information it contains [45].

There are specific privacy and confidentiality issues depending on whether eHealth studies deliver interventions via a web browser on participants' mobile devices versus design a downloadable native application that is able to access information from other applications on the device [13]. If an mHealth application is designed to access the device camera or calendar to help participants track medication and promote an adherence strategy (e.g., the participant is supposed to take a photo of their medication each day or log doses in their calendar), the researcher needs to ensure that only the content the participant wishes to share with the application is collected and stored. Meanwhile, some web browsers enable participants to sync their browsing histories and bookmarks across multiple devices (including one's phone, tablet, and computer), a process participants may not know is occurring. When participants access an intervention on their phone's web browser, other parties could easily find sensitive information or activity on a synched home or office computer by searching the browsing history. To help increase data security, researchers will need to give participants tailored instructions on protecting their own privacy depending on whether they are using a web browser or native application.

Researchers may unintentionally exclude marginalized populations needing interventions the most from HIV research that demands up-to-date mobile devices, raising concerns about social equity in eHealth access. Providing a mobile phone can make interventions more accessible to people who may otherwise be unable to obtain the proper technology, expanding participant eligibility and making study results more generalizable to the entire population [47]. Providing participants with phones also offers advantages for data management and security in eHealth HIV research. For example, program supervisors can ensure the standardization of the phone, with updated security features and HIPAA compliance. Another benefit is that limiting the intervention to one kind of standardized phone system allows developers to comprehensively design and troubleshoot issues on one kind of operating system, rather than trying to spread efforts across coding an intervention that works well across multiple platforms [13]. However, study teams that choose to provide phones need to consider whether the provision of the device actually makes participants safer, with better data and privacy protection, compared with what the participant would otherwise have accessible.

For participants who already have access to phones, developing an intervention that will be compatible with their existing devices increases the likelihood that they will intuitively understand how to navigate the system and thus be more motivated to adhere [13]. The decision of whether to provide a phone within an intervention should thus be considered in this context of usability; whatever protocol is more likely to encourage engagement should be pursued, keeping in mind that for participants without phones, there is zero usability to a potential mHealth intervention.

Informed Consent

Researchers are increasingly aware of the importance of protecting sensitive health data from electronic security breaches. While some teams spend a great amount of time and monetary resources on implementing technological protections, they may fail to devote similar resources to ensuring participants' privacy in everyday use of the intervention.

Social circumstance moderates the severity of risks to participants when researchers do not adequately protect confidentiality. For example, a participant in a society that criminalizes homosexuality or intravenous drug use might face legal consequences if a data breach or privacy violation compromises their confidentiality in an HIV treatment or testing intervention. Likewise, a seropositive woman in a relationship may be vulnerable to intimate partner violence if she unintentionally reveals her status through phone reminders or application use [48]. Sexual and gender minority individuals risk losing their jobs in areas of the USA where employment discrimination against gay and transgender individuals is legal and where discrimination in healthcare settings is common [49–51]. As a consequence, informed consent information must include clear descriptions of the extent and limits of confidentiality protections [10, 52].

eHealth researchers have a responsibility to explain to participants the steps they have taken to protect confidentiality of participant data, such as using secure institutional servers, encryption, and biometric identification, while disclosing the limitations of these measures. For example, when data are stored on third-party networks running survey software or social media sites, researchers cannot guarantee total confidentiality because they do not control the networks [14]. It is particularly important to explain to participants the extent to which third-parties such as social media companies or intervention platforms will have access or ownership to their data, and the limits of researcher control in this regard. If there is potential for data sharing and secondary data analysis by other researchers, informed consent processes must include broad consent language [53]. In eHealth HIV research where data sharing can reveal sensitive participant information, it may be helpful to give participants a comprehension quiz after initially presenting consent materials and then review any aspects of confidentiality protections that were misunderstood before proceeding with the study [12]. Because close to half of eHealth application users stop interacting with the programs shortly after downloading, building privacy safeguards into the application while incentivizing use of the intervention is a crucial balance to strike [54].

Participant-Driven Privacy Measures

Researchers should give participants instructions on actions they can take to protect their own privacy during the eHealth intervention and should make clear the limitations of privacy protections put in place by the study team if participants do not follow these recommendations. For example, researchers in a peer-dyad texting eHealth HIV prevention study implemented a self-safety privacy assessment in the assent/consent phase to ensure that the adolescent participants would be able to follow recommended privacy guidelines if they enrolled [46]. This assessment covered topics such as using a password, deleting cookies, and recognizing when a text recipient has a text-tracking application on their phone. In another study, when participants had to download a secure video chat mobile application for an HIV intervention, research staff showed them how to set up the privacy settings on their phones and make sure that notifications from the app would not show up on their phone lock screens [41]. Additional strategies include recommending that participants create alternate email addresses to login to online interventions so as to remain anonymous or to use one-time passwords or secure links for sending to verified individuals that could only be used one time [8•, 55]. To the extent possible, informing participants about privacy protections and risks should begin at the recruitment stage [8•]. Research teams should advise participants to complete the online screener in private, avoid using a public computer, and clear their browser cache after completing the screener.

Many studies attempt to make it easier or more intuitive for participants to keep information private, reducing demands on their time and effort, while still encouraging the steps they should take to protect their privacy. For example, some studies used trigger-based notification systems, whereby failure to report compliance (that the participant had taken their medication on a given day) resulted in automatic message generation, with the intention of reminding participants who may have forgotten [56]. When the notification schedule is unspecified, the unintended visibility or conspicuousness of electronic reminders can compromise participant privacy when messages appear at inopportune times. To ease the burden, some eHealth HIV medical adherence interventions allowed participants to make choices in regard to the content and timing of reminder messages [4, 47, 55–57]. The extent to which such customization is feasible will be dependent on available formats, as not all participants are able to control notification settings on the phones they have available [2, 58].

Youth or resource-poor individuals who do not reliably have their own cell phones may have to rely on a parent's or partner's device [59]. This presents additional challenges for keeping electronically communicated information relevant to HIV status, behaviors, or treatments confidential. For example, family members sharing devices with the participant might receive timed medication reminders, compromising participant privacy as well as interfering with messaging meant to encourage health maintenance behaviors. In such cases, where there are limits to the intervention team's ability to design sufficient participant protections, the use of eHealth modalities for HIV research may not be ethically appropriate. However, using passwords and pins to restrict access to eHealth HIV-related messaging can somewhat mitigate the risk of exposure on shared phones.

As described earlier in this article, populations at risk for HIV or PLWH who are socially or geographically isolated may benefit greatly from the peer or community support eHealth interventions offer [47]. Examples include chatrooms, social media groups and feeds, online message boards, and text-buddy programs in which users match with peers to provide text-based support. Interaction among multiple users within eHealth interventions brings up new privacy issues that researchers should address during informed consent processes. One way to protect participants' privacy on digital message boards is to require participants to choose a non-identifying username and avatar, which allows for "personalization with anonymity" [60•, 61]. Aliases may not always protect participant privacy if their chosen handles can be traced to other social media or dating accounts, so researchers can mitigate informational risk by ensuring that informed consent procedures communicate the importance of choosing a unique name (compared with other accounts they have online).

Participants who form supportive relationships online through eHealth studies may wish to continue them in-person, which may provide additional social benefit. Although there are concerns among researchers that participants who contact each other outside the survey may engage in unsafe sexual practices and thus increase their sexual risk, follow-up studies on HIV peer interventions facilitated by social media use found this to be rare [35]. Researchers can take steps to protect participants who wish to keep their identities private, but if two consenting adults wish to communicate offline, there is a limit to investigator control in this context.

Researchers may consider the privacy risks for minors to be greater than for adult participants. A text-based intervention that matched youth participants in dyads considered this to be an ethical concern and initially put in place algorithmic controls to prevent participants from exchanging contact information [45, 46]. They found that participants were able to circumvent these systems and the research team had to manually

Table 1 Privacy and confidentiality recommendations for HIV eHealth research teams

Procedure	Researcher Responsibility
Online recruitment	• Be informed as to whether the content of targeted ads or the linked study website may provide third-party companies with potentially stigmatizing information about the participant, including sexual and gender minority identifications, HIV status, or substance use • Be knowledgeable of updates to Terms of Service for third-party services • Select secure servers for sending and receiving recruitment materials • Instruct participants to complete recruitment screeners in private and to delete website links afterwards • Provide peer recruiters with sufficient training and monitoring to protect the privacy of those they recruit through online snowball or respondent-driven sampling • Manually review online validity checks • Be mindful that people at greater risk for or living with HIV may have differing expectations and standards about their online privacy depending on how open they are about their sexual orientation, gender identity, or HIV status, how tolerant the community they live in is, or their general views about how their online data is or should be used
Data maintenance	• Use encryption for transfer of participant data to research servers over cellular data or wireless networks, especially for sensitive information specific to HIV eHealth interventions including HIV medication adherence, tracking of sexual activity, substance use, and mental health logs • Consider whether providing participants with mobile devices will allow researchers a greater degree of ensuring confidentiality of participant data • Implement protocol for remote locking or removal of data from intervention-specific mobile applications in the event of a lost or compromised device • Structure interventions to require additional pins, passwords, or finger-print recognition each time a user wishes to access them • Balance the fact that verification processes that are too cumbersome discourage participants from consistent use with participant desire for protection of sensitive data • Be aware that most smartphone users do not take advantage of comprehensive security features • Involve developers in conversations around usability to ensure integrated security features • In cases such as shared cell phone use, where there are limits to the intervention team's ability to design sufficient participant protections, the use of eHealth modalities for HIV research may not be ethically appropriate
Informed consent	• Conduct initial research on the technological competencies of the target population to help steer proper informed consent procedures • Include a thorough description of the key information participants will need to make a reasoned participation decision based on the extent and limits of confidentiality protections, and use comprehension quizzes to ensure participants understand privacy risks • Provide education or training that promotes appropriate understanding of an intervention's privacy protection features and privacy risk • Include customization options for notification timing and reminder messaging content to help participants better-protect their privacy in eHealth interventions • Implement checkpoints for assessment of harm at every stage of the intervention; make relevant information known to study participants so they can reevaluate their involvement

monitor conversations. Other online peer-intervention studies use algorithms to ensure that online partner matching is limited to individuals separated geographically at distances that discourage in-person meetings [62].

Some peer-based eHealth interventions do not offer anonymity for participants because they require users to use their real social media accounts [17, 36]. Participant feedback from these interventions suggests that some participants worry that their involvement might appear on their friends' newsfeeds [35]. The popularity of different social media platforms among different populations and the way distinct groups use these applications have evolved over the years. For example, adolescent populations favor different social media platforms than adults and may have different comfort levels with engaging with various websites [63]. As with other technological advances, the content of informed consent for HIV eHealth studies will need to reflect how cohort differences influence participants' motivation and ability to protect their online privacy.

Conclusions: The Evolving Nature of eHealth Technologies and Informational Risk

This overview illustrates the many challenges and ways that research teams conducting eHealth HIV intervention studies have employed strategies for online recruitment, data maintenance, and informed consent procedures to minimize informational risk to their participants' identifiable information. Current guidelines provide an ethical framework to internet-based research [9–15, 18, 40], but few are specific to the unique considerations of research involving people at risk for or living with HIV [17, 20]. Below, we summarize the recommendations most relevant to current eHealth research informational risk protections, aware that the dynamic changing nature of technology will require continued modifications (Table 1).

Although this review captures some of the most up-to-date privacy and confidentiality measures used in the field, technological progression is rapid. The proper implementation of research-based interventions can take a great deal of time. This discrepancy in pacing introduces the not-insignificant risk that by the time an eHealth intervention has been rigorously tested and analyzed to be approved for wider use, the technology that supports the intervention may no longer be current [13]. Outdated technologies may not be available for widespread use, interfering with access, both on the side of research teams and participants. That an intervention technology may soon become obsolete changes the calibration of the risk-benefit-analysis.

Potential eHealth participants are assessing their own personal risk-benefit ratio any time they choose whether to engage with an intervention. Some participants may choose to sacrifice digital privacy for the convenience, time-saving, and cost-saving nature of eHealth interventions [64]. The question then becomes not only how to minimize further the risk participants face but the ways in which the potential benefits are maximized. Researchers can outline strategies to communicate meaningful health-related information to participants and consult community advisory boards in every step of the development and implementation process to ensure that the intervention is fulfilling participant expectations. Finally, in the same manner that IRB approval and regulatory compliance are routinely mentioned in research articles, discussion of the specific steps research teams take to protect participant privacy within an intervention should be included in relevant written material.

Conclusion

In conclusion, as indicated by the current review, investigators and IRBs need to be prepared for continuously evolving technological challenges to confidentiality and acquire the competencies to rapidly address these challenges in ways that protect the rights and dignity of participants.

Funding Information This work was supported by NIDA grant R25 DA031608-01, Principle Investigator, C.B.Fisher.

Compliance with Ethical Standards

Conflict of Interest No potential conflicts of interest relevant to this article were reported.

Human and Animal Rights and Informed Consent This article does not contain any studies with human or animal subjects performed by any of the authors.

References

Papers of particular interest, published recently, have been highlighted as:
- Of importance

1. Anderson M, Perrin A, Jiang J, Kumar M. 10% of Americans don't use the internet. Who are they? Pew Res. Cent. 2019. https://www.pewresearch.org/fact-tank/2019/04/22/some-americans-dont-use-the-internet-who-are-they.
2. Dowshen N, Kuhns LM, Gray C, Lee S, Garofalo R. Feasibility of interactive text message response (ITR) as a novel, real-time measure of adherence to antiretroviral therapy for HIV+ youth. AIDS Behav. 2013;17:2237–43. https://doi.org/10.1007/s10461-013-0464-6.
3. Garofalo R, Kuhns LM, Hotton A, Johnson A, Muldoon A, Rice D. A randomized controlled trial of personalized text message reminders to promote medication adherence among HIV-positive adolescents and young adults. AIDS Behav. 2016;20:1049–1059. https://doi.org/10.1007/s10461-015-1192-x.
4. LeGrand S, Knudtson K, Benkeser D, Muessig K, Mcgee A, Sullivan PS, et al. Testing the efficacy of a social networking gamification app to improve pre-exposure prophylaxis adherence (P3: prepared, protected, emPowered): protocol for a randomized controlled trial. JMIR Res Protoc. 2018;7:e10448. https://doi.org/10.2196/10448.
5. Mustanski B, Parsons JT, Sullivan PS, Madkins K, Rosenberg E, Swann G. Biomedical and behavioral outcomes of keep it up!: an ehealth HIV prevention program RCT. Am J Prev Med. 2018;55:151–8. https://doi.org/10.1016/j.amepre.2018.04.026.
6. Holloway IW, Winder TJ, Iii CHL, Tan D, Boyd D, Novak D. Technology use and preferences for mobile phone–based HIV prevention and treatment among black young men who have sex with men: exploratory research. JMIR MHealth Uhealth. 2017;5:e46. https://doi.org/10.2196/mhealth.6436.
7. Saberi P, Siedle-Khan R, Sheon N, Lightfoot M. The use of mobile health applications among youth and young adults living with HIV: focus group findings. AIDS Patient Care STDs. 2016;30:254–60. https://doi.org/10.1089/apc.2016.0044.

8.• Bragard E, Fisher CB, Curtis BL. "They know what they are getting into:" Researchers confront the benefits and challenges of online recruitment for HIV research. Ethics Behav. 2019;1–15. doi: https://doi.org/10.1080/10508422.2019.1692663. **This article reported on the experiences of principal investigators engaged in online HIV research in order to illuminate the scientific and ethical benefits and challenges of online recruitment. Topics include sampling, data integrity, privacy protections and the need for enhanced competencies and resources.**

9. Information security. In: Research ethics and compliance training. CITI Program. https://about.citiprogram.org/en/course/information-security. Accessed 31 Oct 2019.

10. Markham A, Buchanan E. Ethical decision-making and internet research. In: recommendations from the AoIR ethics working committee (version 2.0). 2012. https://aoir.org/reports/ethics2.pdf. .

11. National Institutes of Health: Guidance regarding social media tools. In: Natl. Inst. Health NIH. 2016. https://www.nih.gov/health-information/nih-clinical-research-trials-you/guidance-regarding-social-media-tools. Accessed 28 Oct 2019.

12. SACHRP. Considerations and recommendations concerning internet research and human subjects research regulations. US Department of Health and Human Services. 2016. https://www.hhs.gov/ohrp/sites/default/files/ohrp/sachrp/mtgings/2013%20March%20Mtg/internet_research.pdf. Accessed 31 Oct 2019.

13. Ben-Zeev D, Schueller SM, Begale M, Duffecy J, Kane JM, Mohr DC. Strategies for mHealth research: lessons from 3 mobile intervention studies. Adm Policy Ment Health Ment Health Serv Res. 2015;42:157–67. https://doi.org/10.1007/s10488-014-0556-2.

14. British Psychological Society. Ethics guidelines for internet-mediated research. 2017. https://www.bps.org.uk/news-and-policy/ethics-guidelines-internet-mediated-research-2017. Accessed 31 Oct 2019.

15. Kraut R, Olson J, Banaji M, Bruckman A, Cohen J, Couper M. Psychological research online: report of Board of Scientific Affairs' advisory group on the conduct of research on the internet. Am Psychol. 2004;59:105–17. https://doi.org/10.1037/0003-066X.59.2.105.

16. Gelinas L, Pierce R, Winkler S, Cohen IG, Fernandez Lynch H, Bierer BE. Using social media as a research recruitment tool: ethical issues and recommendations. Am J Bioeth. 2017;17:3–14. https://doi.org/10.1080/15265161.2016.1276644.

17. Young SD. Recommended guidelines on using social networking technologies for HIV prevention research. AIDS Behav. 2012;16:1743–5. https://doi.org/10.1007/s10461-012-0251-9.

18. American Psychological Association. Guidelines for the practice of telepsychology. 2013. https://www.apa.org/practice/guidelines/telepsychology. Accessed 31 Oct 2019.

19. Wrape ER, McGinn MM. Clinical and ethical considerations for delivering couple and family therapy via telehealth. J Marital Fam Ther. 2019;45:296–308. https://doi.org/10.1111/jmft.12319.

20. Chiasson MA, Parsons JT, Tesoriero JM, Carballo-Dieguez A, Hirshfield S, Remien RH. HIV behavioral research online. J Urban Health Bull N Y Acad Med. 2006;83:73–85. https://doi.org/10.1007/s10508-011-9854-x.

21. Muessig KE, Nekkanti M, Bauermeister J, Bull S, Hightow-Weidman LB. A systematic review of recent smartphone, internet and web 2.0 interventions to address the HIV continuum of care. Curr HIV/AIDS Rep. 2015;12:173–90. https://doi.org/10.1007/s11904-014-0239-3.

22. Jones J, Salazar LF. A review of HIV prevention studies that use social networking sites: implications for recruitment, health promotion campaigns, and efficacy trials. AIDS Behav. 2016;20:2772–81. https://doi.org/10.1007/s10461-016-1342-9.

23. Curtis BL. Social networking and online recruiting for HIV research: ethical challenges. J Empir Res Hum Res Ethics. 2014;9:58–70. https://doi.org/10.1525/jer.2014.9.1.58.

24.• Rendina HJ, Mustanski B. Privacy, trust, and data sharing in web-based and mobile research: participant perspectives in a large nationwide sample of men who have sex with men in the United States. J Med Internet Res. 2018;20:e233. doi: https://doi.org/10.2196/jmir.9019. **This study analyzed data from an online sample of gay and bisexual men who have sex with men to examine trust and privacy concerns across different online venues (e.g. universities versus search engines); data usage (e.g. collection by application owners, anonymous selling to third parties, and anonymous sharing with researchers); and different types of data (e.g. public profiles vs. online usage).**

25. Hirshfield S, Downing MJ Jr, Parsons JT, Grov C, Gordon RJ, Houang ST, et al. Developing a video-based eHealth intervention for HIV-positive gay, bisexual, and other men who have sex with men: study protocol for a randomized controlled trial. JMIR Res Protoc. 2016;5:e125. https://doi.org/10.2196/resprot.5554.

26. Mitchell J, Lee J-Y, Stephenson R. How best to obtain valid, verifiable data online from male couples? Lessons learned from an eHealth HIV prevention intervention for HIV-negative male couples. JMIR Public Health Surveill 2016;2:e152. doi: https://doi.org/10.2196/publichealth.6392.

27. Madkins K, Greene GJ, Hall E, Jimenez R, Parsons JT, Sullivan PS, et al. Attrition and HIV risk behaviors: a comparison of young men who have sex with men recruited from online and offline venues for an online HIV prevention program. Arch Sex Behav. 2018;47:2135–48. https://doi.org/10.1007/s10508-018-1253-0.

28. Gutiérrez MA, Quevedo MF, Valle SM, Jacques-Aviñó C, David ED, Caylà JA, et al. Acceptability and effectiveness of using mobile applications to promote HIV and other STI testing among men who have sex with men in Barcelona, Spain. Sex Transm Infect 2018;94:443–448. doi: https://doi.org/10.1136/sextrans-2017-053348.

29. Sun CJ, Stowers J, Miller C, Bachmann LH, Rhodes SD. Acceptability and feasibility of using established geosocial and sexual networking mobile applications to promote HIV and STF testing among men who have sex with men. AIDS Behav. 2015;19:543–52. https://doi.org/10.1007/s10461-014-0942-5.

30. Grindr: Terms of Service. https://www.grindr.com/terms-of-service. Accessed 30 Sep 2019.

31. Bond KT, Ramos SR. Utilization of an animated electronic health video to increase knowledge of post-and pre-exposure prophylaxis for HIV among African American women: nationwide cross-sectional survey. JMIR Form Res. 2019;3:e9995. https://doi.org/10.2196/formative.9995.

32. Grey JA, Konstan J, Iantaffi A, Wilkerson JM, Galos D, Rosser BRS. An updated protocol to detect invalid entries in an online survey of men who have sex with men (MSM): how do valid and invalid submissions compare? AIDS Behav. 2015;19:1928–37. https://doi.org/10.1007/s10461-015-1033-y.

33. Fisher CB, Fried AL, Desmond M, Macapagal K, Mustanski B. Perceived barriers to HIV prevention services for transgender youth. LGBT Health. 2018;5:350–8. https://doi.org/10.1089/lgbt.2017.0098.

34. Mitchell JW. HIV-negative and HIV-discordant gay male couples' use of HIV risk-reduction strategies: differences by partner type and couples' HIV-status. AIDS Behav. 2013;17:1557–69. https://doi.org/10.1007/s10461-012-0388-6.

35. Chiu CJ, Menacho L, Fisher C, Young SD. Ethics issues in social media–based HIV prevention in low-and middle-income countries. Camb Q Healthc Ethics. 2015;24:303–10. https://doi.org/10.1017/S0963180114000620.

36. Patel VV, Ginsburg Z, Golub SA, Horvath KJ, Rios N, Mayer KH, et al. Empowering with PrEP (E-PrEP), a peer-led social media–based intervention to facilitate HIV preexposure prophylaxis adoption among young black and Latinx gay and bisexual men: protocol for a cluster randomized controlled trial. JMIR Res Protoc. 2018;7:e11375. https://doi.org/10.2196/11375.

37. Fuchs JD, Stojanovski K, Vittinghoff E, McMahan VM, Hosek SG, Amico KR, et al. A mobile health strategy to support adherence to antiretroviral preexposure prophylaxis. AIDS Patient Care STDs. 2018;32:104–11. https://doi.org/10.1089/apc.2017.0255.

38. Security rule guidance material. In: Health information privacy. U.S. Department of Health & Human Services. https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html. Accessed 26 Oct 2019.

39. Maiorana A, Steward WT, Koester KA, Pearson C, Shade SB, Chakravarty D, et al. Trust, confidentiality, and the acceptability of sharing HIV-related patient data: lessons learned from a mixed methods study about health information exchanges. Implement Sci. 2012;7:34. https://doi.org/10.1186/1748-5908-7-34.

40. Carter A, Liddle J, Hall W, Chenery H. Mobile phones in research and treatment: ethical guidelines and future directions. JMIR MHealth Uhealth. 2015;3:e95. https://doi.org/10.2196/mhealth.4538.

41. Wootton AR, Legnitto DA, Gruber VA, Dawson-Rose C, Neilands TB, Johnson MO, et al. Telehealth and texting intervention to improve HIV care engagement, mental health and substance use outcomes in youth living with HIV: a pilot feasibility and acceptability study protocol. BMJ Open. 2019;9:e028522. https://doi.org/10.1136/bmjopen-2018-028522.

42. Berkelaar BL, Buzzanell PM. Online employment screening and digital career capital: exploring employers' use of online information for personnel selection. Manag Commun Q. 2015;29:84–113. https://doi.org/10.1177/0893318914554657.

43. Cagle M. Facebook, Instagram, and Twitter provided data access for a surveillance product marketed to target activists of color. In: ACLU North. CA. 2016. https://www.aclunc.org/blog/facebook-instagram-and-twitter-provided-data-access-surveillance-product-marketed-target. Accessed 26 Oct 2019.

44. Smith A, Duggan M. Online dating & relationships. Pew Res. Cent. Internet Sci. Tech. 2013. https://www.pewresearch.org/internet/2013/10/21/online-dating-relationships. Accessed 31 Oct 2019.

45. Li DH, Brown CH, Gallo C, Morgan E, Sullivan PS, Young SD, et al. Design considerations for implementing eHealth behavioral interventions for HIV prevention in evolving sociotechnical landscapes. Curr HIV/AIDS Rep. 2019:1–14.

46. Ybarra ML, Liu W, Prescott TL, Phillips G, Mustanski B. The effect of a text messaging based HIV prevention program on sexual minority male youths: a national evaluation of information, motivation and behavioral skills in a randomized controlled trial of Guy2Guy. AIDS Behav. 2018;22:3335–44. https://doi.org/10.1007/s10461-018-2118-1.

47. Laurence C, Wispelwey E, Flickinger TE, Grabowski M, Waldman AL, Plews-Ogan E, et al. Development of PositiveLinks: a mobile phone app to promote linkage and retention in care for people with HIV. JMIR Form Res. 2019;3:e11578. https://doi.org/10.2196/11578.

48. World Health Organization. 16 ideas for addressing violence against women in the context of HIV epidemic: a programming tool. 2013. https://www.who.int/reproductivehealth/publications/violence/vaw_hiv_epidemic/en. Accessed 31 Oct 2019.

49. Fisher CB, Fried AL, Desmond M, Macapagal K, Mustanski B. Facilitators and barriers to participation in prep HIV prevention trials involving transgender male and female adolescents and emerging adults. AIDS Educ Prev Off Publ Int Soc AIDS Educ.

50. Fisher CB, Fried AL, Macapagal K, Mustanski B. Patient–provider communication barriers and facilitators to HIV and STI preventive services for adolescent MSM. AIDS Behav. 2018;22:1–12. https://doi.org/10.1007/s10461-018-2081-x.

51. Liptak A, Peters JW. Supreme court considers whether civil rights act protects L.G.B.T. workers. N. Y. Times. 2019. https://www.nytimes.com/2019/10/08/us/politics/supreme-court-gay-transgender.html. Accessed 31 Oct 2019.

52. Fisher CB, Oransky M, Mahadevan M, Singer M, Mirhej G, Hodge D. Marginalized populations and drug addiction research: realism, mistrust, and misconception. IRB. 2008;30:1–9.

53. Fisher CB, Layman DM. Genomics, big data, and broad consent: a new ethics frontier for prevention science. Prev Sci. 2018;19:871–9. https://doi.org/10.1007/s11121-018-0944-z.

54. Krebs P, Duncan DT. Health app use among US mobile phone owners: a national survey. JMIR MHealth Uhealth. 2015;3:e101. https://doi.org/10.2196/mhealth.4924.

55. Erguera XA, Johnson MO, Neilands TB, Ruel T, Berrean B, Thomas S, et al. WYZ: a pilot study protocol for designing and developing a mobile health application for engagement in HIV care and medication adherence in youth and young adults living with HIV. BMJ Open. 2019;9:e030473.

56. Ware NC, Pisarski EE, Tam M, Wyatt MA, Atukunda E, Musiimenta A, et al. The meanings in the messages: how SMS reminders and real-time adherence monitoring improve antiretroviral therapy adherence in rural Uganda. AIDS Lond Engl. 2016;30:1287–93. https://doi.org/10.1136/bmjopen-2019-030473.

57. Morano JP, Clauson K, Zhou Z, Escobar-Viera CG, Lieb S, Chen IK, et al. Attitudes, beliefs, and willingness toward the use of mHealth tools for medication adherence in the Florida mHealth adherence project for people living with HIV (FL-mAPP): pilot questionnaire study. JMIR MHealth Uhealth. 2019;7:e12900. https://doi.org/10.2196/12900.

58. Dillingham R, Ingersoll K, Flickinger TE, Waldman AL, Grabowski M, Laurence C, et al. PositiveLinks: a mobile health intervention for retention in HIV care and clinical outcomes with 12-month follow-up. AIDS Patient Care STDs. 2018;32:241–50. https://doi.org/10.1089/apc.2017.0303.

59. Rana Y, Haberer J, Huang H, Kambugu A, Mukasa B, Thirumurthy H, et al. Short message service (SMS)-based intervention to improve treatment adherence among HIV-positive youth in Uganda: focus group findings. PLoS One. 2015;10:e0125187. https://doi.org/10.1371/journal.pone.0125187.

60.• Flickinger TE, DeBolt C, Waldman AL, Reynolds G, Cohn WF, Beach MC, et al. Social support in a virtual community: analysis of a clinic-affiliated online support group for persons living with HIV/AIDS. AIDS Behav 2017;21:3087–3099. doi: https://doi.org/10.1007/s10461-016-1587-3. **This article describes the outcome of a smartphone social support application for a clinic-supported anonymous online group. The authors describe the effectiveness of the intervention as well as the technical issues and interpersonal barriers that limited some participants' full usage.**

61. Muessig KE, Baltierra NB, Pike EC, LeGrand S, Hightow-Weidman LB. Achieving HIV risk reduction through HealthMpowerment.org, a user-driven eHealth intervention for young Black men who have sex with men and transgender women who have sex with men. Digit Cult Educ. 2014;6:164. PMID: 25593616; PMCID: PMC4292870.

62. Ybarra ML, Prescott TL, Phillips GL, Parsons JT, Bull SS, Mustanski B. Ethical considerations in recruiting online and implementing a text messaging–based HIV prevention program with gay, bisexual, and queer adolescent males. J Adolesc Health. 2016;59:44–9. https://doi.org/10.1016/j.jadohealth.2016.03.020.

63. Anderson M, Jiang J. Teens, social media & technology. Pew Res Cent. 2018; https://www.pewresearch.org/internet/2018/05/31/teens-social-media-technology-2018. .

64. Zhou L, Bao J, Watzlaf V, Parmanto B. Barriers to and facilitators of the use of mobile health apps from a security perspective: mixed-methods study. JMIR MHealth Uhealth. 2019;7:e11223. https://doi.org/10.2196/11223.