Appendix: Content Summaries of Selected Best Papers for the IMIA Yearbook 2018, Section Consumer Health Informatics and Education

Bender JL, Cyr AB, Arbuckle L, Ferris LE

Ethics and Privacy Implications of Using the Internet and Social Media to Recruit Participants for Health Research: A Privacy-by-Design Framework for Online Recruitment

J Med Internet Res 2017 Apr 6;19(4):e104

New Internet alternatives are explored by health researchers to recruit people for research studies. The increasing use of social networking sites offers easier access to many kinds of populations. They are also economical and more flexible than former ways. However, the use of social media as an online research recruitment tool raises unique ethical issues regarding knowledge and consent before enrolment. It may pose threats to the principles of Respect for Persons and Concern for Welfare in regard to privacy and the individual's right to control information about him/herself. There is only one known study that describes the ethical challenges of social networking and online recruitment for HIV research which conclusions consisted of a set of recommended best practices for HIV researchers. This paper describes how to use the Internet and social media to recruit cancer patients and their family caregivers for a focus group study on dietary self-management behaviors, the ethical concerns raised by the institutional Research Ethics Board (REB), and the privacy-enhancing strategies developed to address them. Two REB questions were to be answered: "How will you inform users about the potential for privacy breaches and their implications? How will you protect users from privacy breaches or inadvertently sharing potentially identifying information about themselves?" In order to elaborate the social media recruitment strategy, a Privacy by Design (PbD) framework was used. It was developed by the former Information and Privacy Commissioner of Ontario, Canada, in the late 1990s. PbD is based on the following seven foundational principles: (1) Proactive not Reactive, Preventative not Remedial (PbD seeks to anticipate and prevent privacy-invasive events before they happen. PbD does not wait for privacy risks to materialize nor offer remedies after the fact); (2) Privacy as the Default Setting (PbD seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected. No action is required on the part of individuals to protect their privacy. It is built in the system, by default.); (3) Privacy Embedded into Design (PbD is embedded into the design and architecture of the system. It is not bolted on as an add-on, after the fact. Privacy is integral to the system, without diminishing functionality.); (4) Full Functionality — Positive-Sum, not Zero-Sum (PbD seeks to accommodate all legitimate interests and objectives in a positive-sum, win-win manner, not through a dated, zero-sum approach where unnecessary tradeoffs are made.); (5) End-to-End Security — Full Lifecycle Protection (PbD explains that strong security measures are essential to PbD from start to finish. Embedding PbD into the system prior to the first element of information being collected ensures that all data are securely retained throughout the entire lifecycle of the data involved.); (6) Visibility and Transparency — Keep it Open (PbD seeks to assure all stakeholders that whatever the business practice or technology involved, it is, in fact, operating according to the stated promises and objectives, subject to independent verification.); and (7) Respect for User Privacy — Keep it User Centric (PbD requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options). Applying the principles of Privacy by Design made the authors 1) Inform about privacy risks with privacy notices written in plain language and approved by a plain-language expert using familiar words, not jargon, active voice, and a conversational study to convey information clearly. 2) Protect privacy using privacy-enhanced social media messages and 3) Disabling comment features or moderating comments. The authors provide reflection on the perceived privacy risks associated with their social media recruitment strategy and the appropriateness of the risk mitigation strategies they employed by discussing the following: (1) What are the potential risks and who is at risk? (2) Is cancer considered sensitive personal information? (3) What is the probability of online disclosure of a cancer diagnosis in everyday life? and (4) What are the public's expectations for online privacy and their views about online tracking, profiling, and targeting?

Sanderson SC, Brothers KB, Mercaldo ND, Clayton EW, Antommaria AHM, Aufox SA, Brilliant MH, Campos D, Carrell DS, Connolly J, Conway P, Fullerton SM, Garrison NA, Horowitz CR, Jarvik GP, Kaufman D, Kitchner TE, Li R, Ludman EJ, McCarty CA, McCormick JB, McManus VD, Myers MF, Scrol A, Williams JL, Shrubsole MJ, Schildcrout JS, Smith ME, Holm IA

Public Attitudes toward Consent and Data Sharing in Biobank Research: A Large Multi-site Experimental Survey in the US

Am J Hum Genet 2017 Mar 2;100(3):414-27

Biological samples are an increasingly important tool for research on human diseases and their genetic and physiological causes. To ease the storage of and access to biological samples, many are now stored in biobanks. A major ethical problem for prospective biobanks is how to insure participants are given their consent when it is not known what they are consenting to in terms of future research. Biobank investigators and policy makers need help respectively to govern and revise the regulations on the protection of human research subjects. The authors conducted a large survey of attitudes toward consent and data sharing in biobank research among diverse participants recruited at multiple healthcare systems participating in the Electronic Medical Records and Genomics (eMERGE) Network. Individuals were randomly assigned to one of three hypothetical biobank scenarios. The scenarios were identical except for the details regarding consent type and data sharing approach. In the first scenario, donated samples and data could be used for all kinds of medical research

and data could be shared with approved investigators only ("broad-controlled"). The second and third scenarios contained an alternative consent approach or data sharing policy: in the "tiered-controlled" scenario, the consent process allowed participants to select the types of research for which their samples and data could be used, and in the "broad-open" scenario, data sharing policy allowed de-identified data to be shared through an online database open to the public. A multidisciplinary working group of experts defined three relevant sub-domains to be assessed within the overarching domain of "attitudes towards participating in a biobank:" perceived benefits of participating in the described biobank, concerns about participating in the described biobank, and information needs about the governance of the described biobank (e.g., how decisions are made regarding the use of samples and data). Of 90,000 surveys mailed, 7,672 individuals were ineligible due to invalid address, death, or incapacity, and 681 refused to participate. Of the 82,328 eligible individuals, exactly 13,000 responded (response rate 15.8%). Among responders, 11,712 completed the paper (90.1%) and 1,288 the online (9.1%) survey. Overall, 66% (95% CI: 63%–69%) of participants stated that they would be willing to participate in the biobank described to them. Willingness did not differ between broad and tiered consent models (68% versus 66% respectively, P=0.30). Willingness was slightly higher among participants presented with a controlled rather than an open data sharing model, although the difference was not large in absolute terms (68% versus 65%, respectively, P=0.03). Participant characteristics, independently linked with willingness to participate, before attitudes were entered into the model, were: race (as self-reported by the respondents in the survey), education, religiosity, and trust and privacy concerns. When attitudes toward the biobank were entered into the model, each of the three composite scale variables was independently associated with willingness: participants were more willing to participate if they perceived more benefits, had fewer concerns, and had fewer information needs. In this model, education and religiosity remained associated with willingness, but race, trust, and privacy concerns did not. The results from this study suggest that biobanks using broad consent may not be less successful in recruiting participants than if they use more specific consent approaches. Open data sharing may be almost as acceptable to participants as controlled data sharing. Some socio-demographic groups differ in their willingness to participate in biobank research.

Peacock S, Reddy A, Leveille SG, Walker J, Payne TH, Oster NV, Elmore JG

Patient portals and personal health information online: perception, access, and use by US adults

J Am Med Inform Assoc 2017 Apr 1;24(e1):e173-e177

Providing patient online record access has been described as fundamental to patient empowerment. Little is known about the effects of the patient-provider relationship on consumer health information technology acceptance and use. To date, progress has been limited in part by professional resistance and concerns about security and privacy. But research has also found sex, race, and age disparities among patients accessing online personal health information (PHI). The primary objective of this study was to evaluate perspectives and patterns of technology use according to demographic characteristics. Authors used the Health Information National Trends Survey (HINTS) to query participants about their demographic characteristics and their views on the importance of having access to their medical records online, whether the access was offered by a health care provider or online via a patient portal. Of the 3,492 survey participants responding to the three primary online PHI questions, a majority (92%) indicated that they felt access to their PHI online was very or somewhat important; just over a third (34%) reported being offered electronic access to their PHI by their health care provider. Less than a third (28%) reported accessing their own PHI online through a secure website or phone application. Respondents who accessed their own PHI online were significantly more likely to report being offered access by their health care provider (P<.001). Regarding demographic characteristics, there were no differences across race or ethnicity in reported the importance of online access (P=.59 and .67, respectively). However, there were significant differences across race and ethnicity in terms of who was offered access by their health care provider (P=.006 and <.001, respectively) and who accessed their PHI online (P=.041 and <.001, respectively). The authors found that individuals who are older, in poor health condition, poorly educated, and members of ethnic or racial minority groups were less likely to be offered online access or to use a portal access. Just one third of respondents indicated that their health care provider offered them access to their records. Any benefits associated with access to patient portals will be less likely to accrue if not offered and used. Of concern is the finding that health care providers offered access in an inconsistent manner, significantly less often to black and Hispanic individuals than to white and non-Hispanic individuals. Authors conclude that to reduce what appears to be typically defined as the digital divide, health care providers may be key factors affecting current patient electronic access patterns. Encouraging physicians and other health care providers to openly discuss this technology and promote access is vital to ensuring that patients both use and benefit from accessing their PHI online.

Walker DM, Johnson T, Ford EW, Huerta TR

Trust Me, I'm a Doctor: Examining Changes in How Privacy Concerns Affect Patient Withholding Behavior

J Med Internet Res 2017 Jan 4;19(1):e2

Health information technology (HIT) can provide clinicians with more complete patient records at the point of care, enabling better clinical decision-making, facilitating improved care coordination, and insuring patient safety as people move throughout the health care system. HIT can also serve as a tool to enable better patient-provider communication, for example through secure messaging, leading to more patient-centred care. Despite these potential benefits, recent high-profile, EHR security breaches reported in the media make patients wary of this shift to the digital format. This study examined changes in the influence of privacy and secu-

rity concerns on Personal Health Information (PHI) withholding behaviour between 2 time points (2011 and 2014). It was based on the Health Information National Trends Survey (HINTS) which is administered as repeat cross-sections by the National Cancer Institute to a national sample of non-institutionalized adults and gathers information regarding attitudes and perceptions about health information access and use. A prepaid incentive was sent at the first mailing, and multiple follow-ups were sent to recipients in order to maximize the response rate. The total number of respondents in the 2011 and 2014 surveys were 3,959 and 3,677, respectively. For the dependent variable (primary outcome), the HINTS survey asked whether the respondent had "ever kept information from (their) health care provider because (they) were concerned about the privacy and security of (their) medical record" (yes, no). The independent variables were the answer (not at all concerned or confident, somewhat concerned or confident, or very concerned or confident) to the following four questions about privacy and security: do respondents have concerns about unauthorized access to their medical information when it is transferred electronically between providers; do respondents have concerns about unauthorized access to their medical information when it is faxed between health care providers; do they feel confident that safeguards are in place to protect their medical information from unauthorized access; and do they feel confident that they had a say in the collection, use, and sharing of their medical information. Overall, 2,217 respondents from 2011 had complete information and were included in the analytic sample, and 2,176 respondents from 2014 were included. Regarding the dependent variable of interest (whether the respondent had ever withheld any PHI from a medical provider out of privacy or security concerns), no difference was observed between years: in 2011, 14.79% (328/2217) of respondents reported this behavior, whereas in 2014, 14.93% (325/2176) of respondents reported withholding information from their provider out of privacy concerns. The analysis also revealed no changes between 2011 and 2014 in the association of privacy and security attitudes on withholding behaviour. Lastly, there was no effect on respondent confidence that they had some control over their medical information on withholding behavior in either year, and no difference was found between the two years. Overall, the analysis suggests that in spite of the existence of security and privacy concerns, focusing resources on the delivery of high-quality care may be an effective strategy to foster patient trust. Patients may perceive quality as an indicator of a provider's carefulness with their medical information.