HIV status disclosure in a digital age

Advances in information and mobile technologies have heralded great benefits for people living with HIV in recent years. These technologies have improved care, not only in terms of efficient record management, increased uptake of HIV services, and better linkage to care, but also in allowing individuals to take control of their own health. People living with HIV can better manage their access to services and test results, and receive medication reminders through mobile apps such as HIV Testing Sites & Care Services Locator, Every Dose Every Day, and Liverpool HIV iChart.

Social media can be important for providing information and support to those affected by HIV. The advent of gay dating apps in particular has provided opportunities to help normalise discussions about HIV and disclosure of HIV statuses that help to reduce stigma. Indeed, the gay dating and hook-up app Grindr encourages users to reveal their HIV status and has introduced opt-ins to provide testing reminders for the user. A major draw of these apps is the appearance of privacy and confidentiality they provide. However, recent events have cast doubt on the security of committing sensitive data to social media.

In April this year, it was revealed that Grindr had been sharing users' HIV statuses with Apptimize and Localytics, two companies that help organisations optimise their app usage and functionality. Not only were statuses revealed but these data were linked to other information that could reveal users' identities. Although users voluntarily share their HIV status, they do so within the app's gay community of users, and this cannot be construed as permission to disclose their information to third parties. Grindr promotes itself as a responsible gay dating app, yet this incident suggests poor management of sensitive user data. Revelations about Facebook selling data to Cambridge Analytica and data breaches from financial organisations have fuelled an increased scepticism that organisations can be trusted with sensitive information. Grindr's response was that their sharing of data was in line with industry standards. Grindr has since stopped sharing its users' HIV status with other vendors, but this is not the first incident of its kind. In 2015, HZone a dating app for users with HIV, breached the data of nearly 5000 users. It is believed details including user name, email address, and date of birth were left exposed through a reported leaking database.

Not only social media providers but care providers also have a record of poor management of sensitive user information. In 2017, a mailing from CVS Caremark, a US health-care company, might have revealed the status of up to 6000 patients who were receiving HIV medication from Ohio state's AIDS Drug Resistance Program. A reference to HIV was clearly visible in the window of the envelopes used in the mailing. In a strikingly similar incident, AETNA, another US health-care giant, paid around US$17 million to settle a legal challenge after the HIV status of individuals was revealed in a mail-out to patients taking treatment and pre-exposure prophylaxis medication. Up to 12 000 people were affected when again the HIV status of patients was potentially visible in envelope windows.

In the UK, human error was at the centre of another failure to protect patients' privacy and confidentiality. In 2015, the 56 Dean Street sexual health clinic in London sent out an e-newsletter that mistakenly revealed recipients' email addresses to one another. The newsletter was an opt-in service for people using its HIV and other sexual health services, and let people book appointments and receive test results by email. Patients were supposed to be blind-copied into the email but instead details were sent as a group email. Chelsea and Westminster Hospital NHS Foundation Trust who operate the clinic were fined £180 000 by the UK Information Commissioner who said it was a serious breach of the law.

Lessons must be learned from these incidents, but their similarities suggest this is not happening. Better procedures and clear accountability are needed to protect confidentiality. People should at the very least expect to have their privacy protected, and have transparent rights to disclosure, not buried in unclear terms and conditions. Although apps and social media have contributed to the great strides made to counter stigma and discrimination, much still needs to be done. Disclosure without consent might not only result in unnecessary stress, but could have legal and workplace ramifications, and even jeopardise personal safety in some settings.

As much as information and mobile technologies have advanced the lives of thousands of people living with HIV, the basic right to privacy and confidentiality should not be forgotten. ■ *The Lancet HIV*

For more on **Grindr's data sharing** see https://www.buzzfeed.com/azeenghorayshi/grindr-hiv-status-privacy?utm_term=.otdBDDg8Y#.appgppWrZ

For the **official response from Grindr** see https://grindr.tumblr.com/post/172528912083/heres-what-you-should-know-regarding-your-hiv

For more on **HZone** see https://www.databreaches.net/two-apps-with-health-info-found-leaking-researcher-part-2-hzone/

For more on **CVS** see https://edition.cnn.com/2018/04/01/health/cvs-lawsuit-hiv-status-customers/index.html

For more on **AETNA** see https://www.washingtonpost.com/national/health-science/its-in-the-mail-aetna-agrees-to-17m-payout-in-hiv-privacy-breach/2018/01/18/11ed49a2-fc9d-11e7-9b5d-bbf0da31214d_story.html?noredirect=on&utm_term=.5af8d72d4eb5

For more on the **Dean Street story** see http://www.bbc.co.uk/news/technology-36247186 and https://www.theguardian.com/technology/2015/sep/02/london-clinic-accidentally-reveals-hiv-status-of-780-patients