London

stephen.armstrong@me.com

Cite this as: *BMJ* 2024;384:q52

http://dx.doi.org/10.1136/bmj.q52

TECHNOLOGY

What will happen if doctors can't use WhatsApp?

Changes in UK law pose a threat to the security of messaging apps—and therefore their use in the NHS. Patient care will suffer, reports **Stephen Armstrong**

Stephen Armstrong *journalist*

On 13 March 2020 an intensive care specialist sent out a 15 point warning to doctors about the arrival of covid-19: "You will not recognise or prepare fast enough for the sudden influx of critically ill patients, and they will keep coming. Do not underestimate the imminent demise in [patients] . . . very rapid demise . . . 2 metres apart in canteen, stagger breaks. Once you see community spread . . . all health staff wear masks."

Hundreds of NHS staff received these instructions, which were first prepared by a US doctor on the advice of an intensive care specialist in Lombardy, Italy. The warning wasn't delivered by official memo, a team pep talk, or NHS email. It came through WhatsApp.

Mike Grocott, professor of anaesthesia and critical care medicine at the University of Southampton, was a member of four NHS related WhatsApp groups at the time, some with the maximum number of members. He remembers seeing valuable, probably lifesaving, advice about intubation and the possible symptoms or risks arising daily.

In March 2020 as the pandemic took hold, NHS England, the Information Commissioner's Office, the National Data Guardian, and NHS Digital officially allowed clinicians to use messaging services such as WhatsApp "where the benefits outweighed the risk"—reversing years of caution about their use in patient care—provided that the apps used encryption.[1] NHS England latest advice from December 2022 continues that policy, advising healthcare workers to use two step verification and to disable message notifications on the lock screen.[2]

And yet two recent pieces of legislation—one passed, one pending—threaten the use of any end-to-end encrypted messaging (see box) in the NHS.

Ubiquitous—and under threat

Today, some of Grocott's messaging groups have disappeared, and some have evolved. His WhatsApp group for critical care leaders, established in the pandemic, is still active but has become more of a discussion board for managerial issues. And he still uses WhatsApp on the wards: "In day-to-day consulting with colleagues about a patient it's probably easiest to use WhatsApp because it's encrypted," he explains. "You wouldn't be allowed to say 'See Mrs Jenkins in bed 5' on text message."

This use of WhatsApp in the NHS is ubiquitous, says Marcus Baw, an emergency medicine and general practice doctor in Yorkshire. He's in a few clinical WhatsApp groups, including one local emergency locum department that uses the group to send out an alert when there's an urgent need for a locum.

"For all the good and bad, it's a free thing that makes all our lives easier," says Baw. "A lot of the NHS uses WhatsApp and Signal [a similar non-profit app] within teams for operational chitchat rather than specific patient details. It makes it very easy for doctors with the same interests to discuss issues or for those on a rota to discuss rota gaps.

"If it were to disappear, that's a problem from a resilience point of view: we'd have an NHS-wide problem immediately."

The UK's recent Online Safety Act instructs Ofcom, the communications regulator, to monitor user-to-user apps and software, while an amendment to the Investigatory Powers Act in last autumn's King's speech prevents technology companies from introducing new security software or making significant changes to the security of their existing service without the government's approval.

What this means, in effect, is that after a series of consultations and after the Investigatory Powers Act amendment has become law—expected this coming spring—the government will have installed surveillance of all encrypted messaging, making it impossible to be sure that patient information is secure. Furthermore, the app providers—including major tech companies such as Meta (which owns WhatsApp and Facebook), Apple, and Signal—have warned that these new requirements may force them to withdraw services from the UK if it unduly affects their ability to innovate and introduce new security features.

Unusually, says Alan Woodward, visiting professor at the University of Surrey, "the UK has applied extraterritorial rules—meaning that the changes required under the law apply everywhere in the world. But how on earth will they apply a UK law to a US or Chinese company?"

Ross Anderson, professor of security engineering at Cambridge University's Department of Computer Science and Technology, points out that, "as Signal and WhatsApp upgrade their software a number of times a week to deal with bugs or new threats, the UK would have to be treated like Burma or North Korea and simply be avoided rather than wait for approval from GCHQ [Government Communications Headquarters]—which could take months."

The Signal Foundation's president, Meredith Whittaker, says, "The combination of the Investigatory Powers Act reforms and the Online Safety Act presents the possibility of a shocking level of state interference. I think, particularly given the recent cyberattacks on NHS infrastructure, that the risk to patient health and safety and the weakening of the security of medical communications is significant.

"If the choice came down to adulterating the security features that allow us to keep the privacy promises we make to the people who rely on Signal in the NHS or leaving, we would leave."

Ofcom has begun an 18 month consultation on how it will use its new powers under the Online Safety Act, currently timetabled to report back in 2025, and Whittaker says that she's waiting to see the results of this before acting.

Patient care will suffer

"We will use our new online safety powers in a way that's compatible with rights to privacy and freedom of expression," an Ofcom spokesperson tells *The BMJ*. "We won't be reviewing all harmful online material or be able to read private online messages.

"If it's necessary, proportionate, and technically feasible to do so, we'll be able to issue a company with a notice to use accredited technology to deal with child abuse content or terrorism content on their service. Before we'll be able to do that, the government will need to approve and publish minimum standards of accuracy [in the detection of terrorism or child sex abuse content, according to the Online Safety Act], following advice from Ofcom."

The problem with that approach, says Woodward, who has worked in cybersecurity for the government and in the private sector, is that "you either have end-to-end encryption or you don't. There's not some magic dust you can sprinkle so that you only get the bad messages. They all have to be read."

He adds, "Ofcom's problem is that the politicians would very much like client side scanning, which would involve WhatsApp and Signal putting something in their app that sits on every phone and decrypts messages once they arrive. Ofcom knows how unpopular it will be."

What are end-to-end encryption and client side scanning?

Client side scanning is the method that the UK communications regulator, Ofcom, would have to insist on if it could ensure that it could examine potentially harmful messages.

End-to-end encryption of messages involves scrambling the contents of text on a user's phone into a coded message, using a set of rules known as an encryption key. For instance, the key could be simply swapping a letter for a number so that A=1, B=2, and so on. The code can be unscrambled only if the device at the other end has the same set of instructions to decode the message, known as a decryption key.

Because the keys for coding and decoding are stored in the apps on a phone's handset, intercepting a message as it travelled would be useless: it couldn't be decoded without the decryption key.

To have the option to read messages, therefore, Ofcom would need to install software that could read messages after they were written but before they were encrypted—effectively adding surveillance software to every phone in the UK that would be capable of reading every message as it was composed.

Tech companies aren't prepared to subject their apps to this level of government surveillance. If encrypted messaging apps withdraw from the UK, says Grocott, patient care will suffer. "If it's no longer completely private then sharing patient information becomes extremely difficult," he explains. "Sending an imaging report isn't an information governance issue if it's end-to-end encrypted—but, if not, then it is."

Sam Smith, of the patient privacy group MedConfidential, agrees. "Care is better when doctors can talk to each other," he says. "There are some specifically designed medical messaging apps, although many of those that were around before covid have gone bust. And most of those don't interoperate with each other.

"[Imagine] you're the primary doctor in a specialty, and you want to be able to talk to your mate Frederika who's your equivalent at another hospital across town, you know she's on shift and you have her phone number—but the site apps only work on site. For a range of situations doctors find themselves in, only a general app like WhatsApp is easy to use."

Data surveillance risks in healthcare

Woodward points out that once the government can read WhatsApp messages it will be able to overlay the information with data from the Home Office, the Department for Work and Pensions, the electoral roll, and any other government databases. "Once that technology has been built in it could also be used by other governments, to identify dissidents," he explains. "Let's suppose a patient receives medical treatment and a WhatsApp message mentions their name: that could get flagged, and they could be tracked by immigration officials or intelligence agencies."

Primary care has already faced other problems with tech companies' surveillance of messaging apps. In 2022 the *New York Times* reported on two cases in the US where parents using telemedicine had texted pictures of infections in their young children's intimate parts at the request of paediatricians. When the parents' phones automatically uploaded the pictures to their cloud storage accounts, Microsoft's PhotoDNA software flagged them as child sexual abuse material.[3] Google shut down the parents' phones and email accounts and alerted local police, who investigated both parents.

Anderson argues, "If Ofcom finds criteria for spyware that can go into everyone's phone, this is going to make doctor-to-doctor and patient-to-doctor communication susceptible to this sort of problem the whole time.

"For 30 years spooks have been using the threat of kiddie porn and terrorism to get at your phones. The scanning they propose is irrelevant: the majority of sex abuse is in the family. Dealing with that is about a local response, not sweeping population surveillance."

For Baw, the entire problem could have been avoided if the NHS weren't being failed by its IT leaders. "The big picture stuff has been ignored by the people who could have had the vision to say, 'We're the second largest employer in the world, we have the scale to build our own end-to-end encrypted NHS approved app linked to NHS mail,'" he says. "They can't get beyond the idea that tech is too hard and expensive. With £20m and six months, I guarantee that you could build an NHS equivalent."

Grocott says that the convenience of WhatsApp isn't easy to replicate. "We could have an end-to-end encrypted system that was part of the NHS—but WhatsApp is very convenient and works," he explains. "The time it takes to log into your own login on a computer or phone, and then into a particular application with its own login, isn't trivial when compared with looking at my phone and opening WhatsApp."

Baw's hope, however, is that someone in government will realise the electoral foolishness of these two pieces of legislation. "The tech companies are serious," he says. "Can you imagine the outcry from the population if WhatsApp withdraws from the UK? It would be an act of catastrophic self-harm by any government. Perhaps, for once, common sense will prevail.”

Competing interests: Stephen Armstrong is a journalist and author. He is paid to write about technology, medicine, science, politics, and culture for *Wired*, the *Sunday Times*, and the *Daily Telegraph*, among others. He has written books on the private security industry, the rise of oligarchs in the developing world, and poverty in the UK. He is a trustee of the Orwell Foundation and a fellow of the Royal Society of Arts. He owns no stock options or shares in any pharmaceutical, IT, or healthcare companies. He has a personal pension, which may invest in these types of companies.

Provenance and peer review: Commissioned, not externally peer reviewed.

1 Downey A. Clinicians told they can use WhatsApp to share data in face of covid-19. *Digital Health* 2020 Mar 20. https://www.digitalhealth.net/2020/03/clinicians-told-they-can-use-whatsapp-to-share-data-in-face-of-covid-19/

2 NHS England. Using mobile messaging. 20 Dec 2022. https://transform.england.nhs.uk/information-governance/guidance/use-mobile-messaging-software-health-and-care-settings/

3 Hill K. A dad took photos of his naked toddler for the doctor. Google flagged him as a criminal. *New York Times* 2022 Aug 21. https://www.nytimes.com/2022/08/21/technology/google-surveillance-toddler-photo.html