Headline: Opinion: Privacy risks climb in era of big data

Subhead: With telemedicine in its infancy, now is the time to strengthen patient privacy laws

By Kris Alman

Last week, Anthem Blue Cross crossed a high-water mark. Some [80 million patients](http://www.forbes.com/sites/danmunro/2015/02/05/health-data-breach-at-anthem-is-a-blockbuster-could-affect-80-million/)[[1]](#footnote-1) were left adrift after cybercriminals breached Anthem’s database, putting them at risk for [identity theft](http://www.latimes.com/business/la-fi-anthem-hacked-20150204-story.html#page=1)[[2]](#footnote-2). 80 million [exceeds the previous five years of data breaches combined](http://www.forbes.com/sites/danmunro/2014/09/28/is-anyone-really-hipaa-compliant-in-healthcare/)[[3]](#footnote-3) and recorded at the Health and Human Services Office for Civil Rights [data breach hall of shame](https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf).[[4]](#footnote-4)

One might question what it really means to be “HIPAA compliant.”

Data = $$$ in e-health. The ‘P’ in HIPAA isn’t for privacy. It’s for (P)ortability—the kind that (H)ealth (I)nsurance companies need to make sure Big Money flows through America’s fragmented health care “system.” Who takes (A)ccountability for safeguarding our health data if we don’t know where our data flows? Like small tributaries to rivers that eventually feed into oceans, Big Data/Big Money emerges from little data/little money tributaries.

We need dams to control the flow of data, especially when new technology releases a new digital stream. [Senate Bill 144](https://olis.leg.state.or.us/liz/2015R1/Downloads/MeasureDocument/SB144)[[5]](#footnote-5) could create a digital flood. This bill stipulates requirements for health plans to cover telemedical services.

[Telemedical services](https://www.oregonlegislature.gov/bills_laws/lawsstatutes/2013ors743A.html)[[6]](#footnote-6) in Oregon are “delivered through a two-way video communication” which allows a health professional to interact with patients in the comforts of their home… or work… or anywhere their mobile device may be. Last year, Oregon insurance companies and hospitals [killed a similar bill](https://www.thelundreport.org/content/hospitals-along-providence-and-regence-stop-bill-requiring-telemedicine-payments),[[7]](#footnote-7) threatened by ZoomCare—which had already cornered the paying customers market in the Portland metro. [ZoomCare](https://www.zoomcare.com/info/services-prices)[[8]](#footnote-8) currently charges patients $85 cash for Skype [TakeOut®](https://www.zoomcare.com/content/online-visits).

**Google Ventures into healthcare**

The ZoomCare/Skype dynamic duo has a new competitor in Oregon: [Doctor on Demand](http://venturebeat.com/2014/08/06/branson-venrock-others-bet-21m-on-doctor-on-demand-telemedicine-platform/)[[9]](#footnote-9). [Dr. Phil](http://www.drphil.com/)[[10]](#footnote-10) and his son, Jay (executive producer of [*The Doctors*](http://www.thedoctorstv.com/)*[[11]](#footnote-11)*), have teamed up with [Jonathan Bush](https://en.wikipedia.org/wiki/Jonathan_S._Bush)[[12]](#footnote-12) (nephew of George H.W., and President/CEO of [athenahealth](http://newsroom.athenahealth.com/phoenix.zhtml?c=253091&p=irol-newsArticle&ID=2012969),[[13]](#footnote-13) a “leading provider of cloud-based services and mobile applications for medical groups and health systems”) and deep-pocketed venture capitalists: Andreessen Horowitz, Venrock, Lerer Ventures, Shasta Ventures and Google Ventures.

[Google Ventures](http://www.gv.com/about) says it will provide “unparalleled support in design, recruiting, marketing, and *more*” to the [portfolio](http://www.gv.com/portfolio/)[[14]](#footnote-14) of companies it invests in. [Andreessen Horowitz](https://en.wikipedia.org/wiki/Andreessen_Horowitz) is a $4 billion venture capital firm. Marc Andreessen and Ben Horowitz were criticized for investments in Skype that were deemed risky because of feared competition from Google and Apple. When Microsoft acquired [Skype](http://www.wired.com/2011/05/microsoft-buys-skype-2/)[[15]](#footnote-15) in 2011 for $8.5 billion their bet paid off. Their partnership with Google is a brilliant move.

Whether the “*more*” that Google Ventures supports is *lawful* is another thing. Google Ventures’ portfolio includes [Recorded Futures](https://www.recordedfuture.com/)[[16]](#footnote-16), a [joint investment with the CIA](http://www.wired.com/2010/07/exclusive-google-cia/)[[17]](#footnote-17). [Google relies on advertising](https://en.wikipedia.org/wiki/AdSense)[[18]](#footnote-18) to monetize its [“free”](http://www.google.com/policies/technologies/ads/)[[19]](#footnote-19) services by using “cookies.”

In a [lawsuit against Google](http://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=1366&context=historical),[[20]](#footnote-20) students claim Google violated federal and state wiretap laws by intercepting electronic Gmail messages and data-mining those messages for advertising-related purposes–including the building of “surreptitious user profiles.” Judge Lucy Koh, whose jurisdiction is in the heart of Silicon Valley, denied a motion from Google to dismiss the case entirely. She [rejected the company’s argument](http://www.bloomberg.com/news/2014-01-28/google-loses-bid-for-appeals-review-of-gmail-wiretap-suit.html)[[21]](#footnote-21) that Gmail users agreed to let their messages be scanned when they accepted subscription service terms and privacy policies.

Snowden revelations showed the [National Security Agency secretly piggybacked Google cookies](http://www.washingtonpost.com/blogs/the-switch/wp/2013/12/10/nsa-uses-google-cookies-to-pinpoint-targets-for-hacking)[[22]](#footnote-22) for surveillance and to track targets. Skype worked also [with the NSA](http://www.inquisitr.com/843787/snowden-skype-and-microsoft-cooperated-in-nsa-surveillance/); and while it’s still uncertain whether Skype protects [end-to-end encryption](https://www.eff.org/deeplinks/2014/11/scorecard-update-we-cannot-credit-skype-end-end-encryption),[[23]](#footnote-23) Skype [stored videoconferencing communications](http://hbpub.vo.llnwd.net/o16/video/olmk/holt/greenwald/NoPlaceToHide-Documents-Uncompressed.pdf) for the NSA.

**Televangelists unite**

[Dr. Phil](https://www.youtube.com/watch?v=1tf7NOwPrSA),[[24]](#footnote-24) hawking Doctor on Demand services for UTIs, flu and psychotherapy on [YouTube](https://en.wikipedia.org/wiki/YouTube)[[25]](#footnote-25) (a subsidiary of Google since 2006), must have faith that HIPAA security rules won’t be a barrier to their business plan. He says they are going to have “some type of storage of information”—which is concerning since federal law specifically protects [psychotherapy notes](http://www.law.cornell.edu/cfr/text/45/164.508)[[26]](#footnote-26) from unauthorized use or disclosure.

Dr. Phil and his business associates must have felt solace when fellow health televangelist Dr. Oz and his “[NY Med](http://abc.go.com/shows/ny-med)” TV crew fought a lawsuit for [broadcasting a man’s death](https://www.propublica.org/article/when-a-patients-death-is-broadcast-without-permission)[[27]](#footnote-27) without his or his family’s consent. The show’s attorneys argued, *“*(T)he law prohibits medical professionals from sharing information about a patient only after he has been examined or treated.” “After” is the operative word.

Doctor on Demand’s terms of use states, “We will maintain the privacy of your Health Information as required by HIPAA and the regulations promulgated under that Act. We may also use your health information to: Assist in specialized government functions such as national security, intelligence and protective services.”

It further states:

*Google Analytics collects only the IP address assigned to you on the date you visit the Site, rather than your name or other personally identifying information.  Although Google Analytics plants a persistent Cookie on your web browser to identify you as a unique user the next time you visit the Site, the Cookie cannot be used by anyone but Google.  Google’s ability to use and share information collected by Google Analytics about your visits to the Site is restricted by the Google Analytics Terms of Use and the Google Privacy Policy.*

[“Persistent cookies”](http://www.webopedia.com/TERM/P/persistent_cookie.html)[[28]](#footnote-28) identify information about the user, such as Web surfing behavior or user preferences for a specific Web site. In contrast to a [“session cookie”](http://www.webopedia.com/TERM/S/session_cookie.html),[[29]](#footnote-29) persistent cookies are stored on the hard drive until the user deletes the cookie.

Skype’s [privacy policy](http://www.skype.com/en/legal/privacy/),[[30]](#footnote-30) on the other hand, doesn’t even mention HIPAA.

**Telehealth security holes and HIPAA compliance**

The [Telehealth Alliance of Oregon](http://www.ortelehealth.org/content/privacy-and-security-0)[[31]](#footnote-31) references a white paper from the Center for Telehealth and e-Health law. “As defined in the Security Rule, ePHI (Protected Health Information)… does not include paper-to-paper faxes, video teleconferencing, or messages left on voice mail—because the information being exchanged did not exist in electronic form prior to the transmission.”

SB 144 stipulates: “The application and technology used to provide the health service meet all standards required by state and federal laws governing the privacy and security of protected health information.”

Would telemedicine in Oregon be HIPAA compliant for security? When the HIPAA Security Rule excludes the need for business associates to provide secure transmission for teleconferencing, sure!

But even if the bill’s language is amended to specifically include teleconferencing, shouldn’t the bill mandate end-to-end encryption and [other protections](http://www.technologyreview.com/view/535111/encryption-wouldnt-have-stopped-anthems-data-breach/)?

Regardless, Doctor on Demand venture capitalists are betting patients will charge $40 to their credit card for digital urgent care—even if it’s not coved by insurance. Just launch your Chrome browser and paste their web address into Chrome. Or if you prefer, you can [download an app](https://patient.doctorondemand.com/patient/non_chrome/) from the Apple App Store or Google Play and use your smart phone!

Just don’t expect a face-to-face appointment unless you have plenty of frequent flyer miles. The doc-in-a-computer-box most likely does not live in Oregon, let alone have a license to practice here.

I called the Doctor on Demand patient support number. When nobody answered, I called doctor support and talked to a representative. He told me I could immediately get appointments with either Dr. Christopher Pedersen or Dr. Kristin Dean. [Dr. Pederson](https://techmedweb.omb.state.or.us/Clients/ORMB/Public/VerificationDetails.aspx?EntityID=1476978)[[32]](#footnote-32) (who lives in Las Vegas, Nevada) received an Oregon telemedicine license on 12/23/14. Dr. Dean lives in California[[33]](#footnote-33) where she is licensed to practice medicine -- but she is not licensed in Oregon, which may [violate Oregon law](http://library.fsmb.org/pdf/grpol_telemedicine_licensure.pdf)[[34]](#footnote-34).

**There will be fines**

Last year, New York-Presbyterian Hospital and Columbia University Medical Center (the same hospitals where [*NY Med*](http://en.wikipedia.org/wiki/NY_Med)*[[35]](#footnote-35)* is filmed) were [fined a record $4.8 million](http://www.healthcareitnews.com/news/group-slapped-record-hipaa-fine)[[36]](#footnote-36) to settle HIPAA violations. HHS OCR performed its first piloted [HIPAA audit](http://www.hcca-info.org/Portals/0/PDFs/Resources/Conference_Handouts/Compliance_Institute/2014/tue/710print2.pdf)[[37]](#footnote-37) in March 2014. 58 of 59 [covered entities](http://www.emrsoap.com/wp-content/uploads/2013/06/covered-entity.png)[[38]](#footnote-38) had at least one negative finding. In 2015, HHS OCR will shift their focus will to [business associates](https://www.teachprivacy.com/alarming-fact-hipaa-audits/).[[39]](#footnote-39) While there is no private right of action (i.e. no civil lawsuits) for HIPAA violations, individuals *have* successfully sued for [negligence](https://www.teachprivacy.com/lawsuits-hipaa-violations-beyond-journey-rabbit-hole/).[[40]](#footnote-40)

In contemplating the Anthem breach, [Dan Munroe a contributor to *Forbes*](http://www.forbes.com/sites/danmunro/2015/02/05/health-data-breach-at-anthem-is-a-blockbuster-could-affect-80-million/)[[41]](#footnote-41) recommends, “Healthcare enterprises need to establish airtight policies for encrypting all data both in transit and at rest.” He quotes Linn Freedman (who practices data privacy and security law with Nixon Peabody, LLP): “*When OCR (Office of Civil Rights) begins enforcing HIPAA and levies hefty fines and penalties against business associates, they will wake up quickly. In the meantime, patients’ health information is at risk and I have seen a dramatic increase in breaches caused by business associates which have not implemented measures to comply with HIPAA’s  Security Rule.”*

Maybe it’s just me, but I don’t know how you could ever pin data breaches on Google. After all, their [mission](https://www.google.com/about/company/)[[42]](#footnote-42) is to “organize the world’s information and make it universally accessible and useful.”

Oregon telemedicine is in its infancy. We should urge Oregon lawmakers to strengthen state and federal laws to assure patients that their telemedicine visits will be confidential *before* more data dams are breached.

1. http://www.forbes.com/sites/danmunro/2015/02/05/health-data-breach-at-anthem-is-a-blockbuster-could-affect-80-million/ [↑](#footnote-ref-1)
2. http://www.latimes.com/business/la-fi-anthem-hacked-20150204-story.html#page=1 [↑](#footnote-ref-2)
3. http://www.forbes.com/sites/danmunro/2014/09/28/is-anyone-really-hipaa-compliant-in-healthcare/ [↑](#footnote-ref-3)
4. https://ocrportal.hhs.gov/ocr/breach/breach\_report.jsf [↑](#footnote-ref-4)
5. https://olis.leg.state.or.us/liz/2015R1/Downloads/MeasureDocument/SB144 [↑](#footnote-ref-5)
6. https://www.oregonlegislature.gov/bills\_laws/lawsstatutes/2013ors743A.html [↑](#footnote-ref-6)
7. https://www.thelundreport.org/content/hospitals-along-providence-and-regence-stop-bill-requiring-telemedicine-payments [↑](#footnote-ref-7)
8. https://www.zoomcare.com/info/services-prices [↑](#footnote-ref-8)
9. http://venturebeat.com/2014/08/06/branson-venrock-others-bet-21m-on-doctor-on-demand-telemedicine-platform/ [↑](#footnote-ref-9)
10. http://www.drphil.com/ [↑](#footnote-ref-10)
11. http://www.thedoctorstv.com/ [↑](#footnote-ref-11)
12. https://en.wikipedia.org/wiki/Jonathan\_S.\_Bush [↑](#footnote-ref-12)
13. http://newsroom.athenahealth.com/phoenix.zhtml?c=253091&p=irol-newsArticle&ID=2012969 [↑](#footnote-ref-13)
14. http://www.gv.com/portfolio/ [↑](#footnote-ref-14)
15. http://www.wired.com/2011/05/microsoft-buys-skype-2/ [↑](#footnote-ref-15)
16. https://www.recordedfuture.com/ [↑](#footnote-ref-16)
17. http://www.wired.com/2010/07/exclusive-google-cia/ [↑](#footnote-ref-17)
18. https://en.wikipedia.org/wiki/AdSense [↑](#footnote-ref-18)
19. http://www.google.com/policies/technologies/ads/ [↑](#footnote-ref-19)
20. http://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=1366&context=historical [↑](#footnote-ref-20)
21. http://www.bloomberg.com/news/articles/2014-01-28/google-loses-bid-for-appeals-review-of-gmail-wiretap-suit [↑](#footnote-ref-21)
22. http://www.washingtonpost.com/blogs/the-switch/wp/2013/12/10/nsa-uses-google-cookies-to-pinpoint-targets-for-hacking [↑](#footnote-ref-22)
23. https://www.eff.org/deeplinks/2014/11/scorecard-update-we-cannot-credit-skype-end-end-encryption [↑](#footnote-ref-23)
24. https://www.youtube.com/watch?v=1tf7NOwPrSA [↑](#footnote-ref-24)
25. https://en.wikipedia.org/wiki/YouTube [↑](#footnote-ref-25)
26. http://www.law.cornell.edu/cfr/text/45/164.508 [↑](#footnote-ref-26)
27. https://www.propublica.org/article/when-a-patients-death-is-broadcast-without-permission [↑](#footnote-ref-27)
28. http://www.webopedia.com/TERM/P/persistent\_cookie.html [↑](#footnote-ref-28)
29. http://www.webopedia.com/TERM/S/session\_cookie.html [↑](#footnote-ref-29)
30. http://www.skype.com/en/legal/privacy/ [↑](#footnote-ref-30)
31. http://www.ortelehealth.org/content/privacy-and-security-0 [↑](#footnote-ref-31)
32. <https://techmedweb.omb.state.or.us/Clients/ORMB/Public/VerificationDetails.aspx?EntityID=1476978> [↑](#footnote-ref-32)
33. https://www.breeze.ca.gov/datamart/searchLicTypeByName.do?direct=true [↑](#footnote-ref-33)
34. http://library.fsmb.org/pdf/grpol\_telemedicine\_licensure.pdf [↑](#footnote-ref-34)
35. http://en.wikipedia.org/wiki/NY\_Med [↑](#footnote-ref-35)
36. http://www.healthcareitnews.com/news/group-slapped-record-hipaa-fine [↑](#footnote-ref-36)
37. http://www.hcca-info.org/Portals/0/PDFs/Resources/Conference\_Handouts/Compliance\_Institute/2014/tue/710print2.pdf [↑](#footnote-ref-37)
38. http://www.emrsoap.com/wp-content/uploads/2013/06/covered-entity.png [↑](#footnote-ref-38)
39. https://www.teachprivacy.com/alarming-fact-hipaa-audits/ [↑](#footnote-ref-39)
40. https://www.teachprivacy.com/lawsuits-hipaa-violations-beyond-journey-rabbit-hole/ [↑](#footnote-ref-40)
41. http://www.forbes.com/sites/danmunro/2015/02/05/health-data-breach-at-anthem-is-a-blockbuster-could-affect-80-million/ [↑](#footnote-ref-41)
42. https://www.google.com/about/company/ [↑](#footnote-ref-42)