

# PHRs and the Next HIPAA

Reid Cushman, PhD  
Director of Operations, Medical Information Technology  
Project Health Design ELSI Team  
University of Miami

*This document may be used freely for non-commercial purposes  
with appropriate attribution to the source.*

In the US, many federal and state laws condition the treatment of personal health information. But HIPAA is the 440-pound gorilla in the regulatory zoo, and it's been natural to ask how HIPAA might apply to health information in the many flavors of personal health records (PHRs) now emerging. Major information technology sector players like Google and Microsoft, vendors of institutional electronic medical records (EMRs), insurance carriers, employers and scores of others have combined to produce more than 100 PHR offerings so far.

The unfortunate answer to the HIPAA-and-PHR question is: maybe it does, maybe it doesn't. It depends on the details of the implementation, specifically the degree to which the PHR's content "touches" the institutions already covered by HIPAA. We discuss the details that affect the answer below, in the next sections of this paper.

Whatever the details, it's an easy enough matter to "fix." A next version of HIPAA – call it "HIPAA2" – could explicitly include PHRs within its embrace. The hard question is how best to do that, so as to maximize the potential contributions of PHRs to health outcomes, while still giving weight to other valuable things like information security and privacy. Tentative answers to the harder question occupy the last part of this paper.

## PHR TYPES AND INSTITUTIONAL RELATIONSHIPS

It's worth reiterating first what the term PHR embraces, as it is now being applied to a spectrum of possible technical platforms.

At one end of the technical continuum are simple, stand-alone "my health record on a USB stick" implementations created entirely by the data subject's efforts. In this form, PHRs are little different from any other personal record, such as copies of one's bank account numbers. They might be based on data provided by an institution (e.g., one's bank), but the transcription is unique to the individual and might best be labeled a "personal memory aid." Indeed, the implementation need not be electronic. One could argue that a list of medications and major family medical events rendered on a 3x5 card merits inclusion in the family of PHRs just as much.

At the other end of the technical spectrum are comprehensive personal health data collections synchronized with institutional electronic medical records (EMRs), thus potentially containing data from both the data subject and conventional institutional data-system sources. The "original" and multiple backup copies of the EMR would exist within the various source healthcare institutions' control. Those institutional copies might well also include the data that patients themselves have added or aggregated on their own -- entered "manually" or via supplemental data capture devices worn on the person or where they live.

Indeed, it is to the patient's benefit that the institutions provide this service, since if the PHR has valuable data that is not easily replicated then a backup is surely in order. However, data availability and integrity is not the only value in play. To the extent the patient cares about confidentiality, however, the institution's service is not beneficial – it adds another place from which the data may "leak."



This particular technical implementation spectrum is among the factors conditioning the answer to “does HIPAA apply?” Anything within a conventional health care institution’s data collection surely does, and so, presumably, does any copy of data that the patient “authored.” If the data collection “backup” is maintained by an institution that has not conventionally been part of the health data stream – a Microsoft or a Google, say – then the picture is much less clear. To clarify what is clear and what is not, it’s worth revisiting the scope of HIPAA.

## WHAT IS COVERED BY HIPAA?

The content of PHRs would certainly be within the reach of HIPAA. Under its provisions, any health information that is, or reasonably could be, linked to an individual is [protected health information](#) -- in HIPAA-speak, simply "PHI." HIPAA defines PHI very broadly as anything related to the "past, present or future physical or mental health condition" of a person. Only fully [de-identified](#) health information is excluded – where every explicit identifier of a person has been removed, as well as data that could potentially establish identity via statistical techniques.

Note that HIPAA’s [Privacy Rule](#) applies to PHI in "any form or medium." (This is in contrast to HIPAA’s [Security Rule](#), which applies only to PHI in electronic form.) So the Privacy Rule includes paper records as well as electronic ones, faxes, emails, exchanges in phone conversations, and even just talking face-to-face. If it’s health data and it’s identifiable, it’s covered.

## WHO IS COVERED BY HIPAA?

“Anything related” to past, present or future health would potentially sweep in almost everything one might imagine about a person. The limiting question is not the “what” of PHRs, but the “who” – that is, what sorts of natural or legal “person” are within HIPAA’s reach.

HIPAA defines as [covered entities](#) within its reach the following major groups:

- health care providers (e.g., physicians);
- health care facilities (hospitals, clinics, physician offices);
- health plans (HMOs, insurers); and
- health information clearinghouses<sup>1</sup>

On a broad reading, that puts almost every US organization that provides or pays for health services, or exchanges health data of any kind with such entities, within the reach of HIPAA. HIPAA reaches even to the [business associates](#) that handle health data on a covered entity’s behalf.

## DO PHRs INVOLVE “CLEARINGHOUSES”?

Individuals, unless they happen to be health care practitioners, are not covered entities. A PHR conceived as a stand-alone “health data on a USB stick” repository would appear to be outside the realm of covered entities. However, almost no one with ambitions for PHRs wants to leave them at this level, for the reasons outlined above.<sup>2</sup> Ensuring the integrity and availability of PHR data whenever and wherever a patient may need access to it requires both backup copies and a communications platform to reach those backups.

That need has led to the emergence of a myriad of players providing a PHR “repository” service. The most recent major entrant is Microsoft’s “[HealthVault](#),” with the emergence of arch-rival Google’s “Google Health” soon to follow.

Providing an “anywhere, anytime” Internet portal to PHR data is only the beginning. Robust functionality for PHRs requires the ability to exchange their data with the parties that provide health services to the

patient – e.g., physicians in clinics, hospitals, pharmacies. Hence sources like Health Vault feature the capacity to “catalog existing health records, receive test results, or monitor current physical readings.” If any of the sources or destinations of such information is a covered entity – and it is hard to see how they would not be – then the PHR service appears to be functioning as a health information clearinghouse.

Repository providers like HealthVault promise that “[y]ou decide who can see and use your information on a case-by-case basis” and that any recipients of such data must, as a condition of participation, agree “not to disclose your data without your express consent.” If HealthVault is a covered entity, that cannot be true. HIPAA allows – indeed, requires – many types of information disclosure without the data subject’s permission (see next section). HealthVault navigates around this problem in its Privacy Statement (emphasis supplied):

“Microsoft may access and/or disclose your personal information if we believe such action is necessary to: (a) comply with the law or legal process served on Microsoft; (b) protect and defend the rights or property of Microsoft (including the enforcement of our agreements); or (c) act in urgent circumstances to protect the personal safety and welfare of users of Microsoft services or members of the public.”

### **SHOULD PHRs BE COVERED BY HIPAA?**

Whether PHRs are covered by HIPAA is a question ultimately for the regulatory enforcers of HIPAA (the Office of Civil Rights in the US Department of Health and Human Services), the federal courts – or for Congress, should it choose to add a paragraph or two to amend HIPAA. Whether it should be covered is a harder question.

There can be no doubt that HIPAA’s security provisions have had a beneficial effect on the health sector, forcing covered entities to attend to data protection in a more focused manner. The balance for privacy is a harder call, since HIPAA has formalized the rules of information exchange to a much greater degree, but the rules it has formalized allow a great deal of sharing of information.

HIPAA allows uses and disclosures without consent for a broad range of purposes, including transactions related to [treatment](#), [payment](#), and a broad range of other core [health care operations](#). Neither does HIPAA require specific permission for a broad range of activities required by law, including [public health](#) and [health system oversight](#) activities, reporting about victims of [abuse, neglect or domestic violence](#), content for [judicial and administrative proceedings](#), and activities related to “specialized government functions” like [national security](#), [military and veterans activities](#), [corrections](#) and [law enforcement](#), or anything required to avert a serious, imminent threat to public safety. HIPAA does require a signed permission (called an “authorization”) for many – but decidedly not all – uses or disclosures for [research](#), [marketing](#) and [fundraising](#).<sup>3</sup>

In other words, when it comes to consent in HIPAA, the exceptions are the rule. Would a similar breadth of allowed uses and disclosures without consent have a chilling effect on PHRs? That would depend on whether the parameters of accessibility, by type of information and type of use, could be crafted in a way that satisfied both data subjects and the constituencies of potential data users. The experience with HIPAA to date demonstrates how difficult a task that is. For persons who elevate privacy above all else, the only safe PHR is one that is delinked from any institutional data sources or support. That sacrifices a great deal of a PHR’s potential,<sup>4</sup> but it may be a tradeoff that some persons wish to make.

It is certainly not irrational to prefer to keep information out of institutional records if you can’t control its use and it can be used to hurt you – a rationality that applies to PHRs if that content will reappear in institutional backups. However, providing a strong consent model for PHRs is not without costs. The information in such records may have social value, for all the reasons that institutional health records have value. Making PHRs attractive from a personal privacy perspective trades off that value, though in ways that are obviously extremely difficult to quantify.<sup>5</sup>

## ACKNOWLEDGEMENTS

Michael Froomkin of the UM ELSI team contributed to this paper.

## NOTES

---

<sup>1</sup> More expansively, definitions of covered entities at [45 CFR 160.103](#) and [45 CFR 164.501](#) include:

- *health plan* means any individual or group plan that provides, or pays the cost of, medical care -- including public and private health insurance issuers, HMOs or other managed care organizations, employee benefit plans, the Medicare and Medicaid programs, military/veterans plans, and any other "policy, plan or program" for which a principal purpose is to provide or pay for health care services;
- *health care provider* means a provider of medical or health services, and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business; and
- *health care clearinghouse* means a public or private entity, including a billing service, repricing company, community health information system, and "value-added" networks and switches, that either processes or facilitates the processing of health information.

The last of these is further qualified by whether "the business or agency processes or facilitates the processing of health information from nonstandard format or content into standard format" or vice-versa.

See also [Covered Entity Charts \(DHHS\)](#).

<sup>2</sup> Attempting to apply a HIPAA-like regime to privately created and privately held health data raises a number of difficult legal issues that both Congress and the courts are likely to try to avoid. As a practical matter, the disclosure and consent issues arise only when that data is disclosed to a health-care provider or to a third party such as HealthVault – but then they arise with a vengeance.

<sup>3</sup> If a repository service like HealthVault is considered a clearinghouse, one response would be for the covered entity to secure a business associate contract before transferring information to it. Alternatively, covered entities could require the patient's specific authorization for single or on-going transfers to any PHR repository.

<sup>4</sup> Google Health includes the SafeMed Analysis Engine to weigh symptoms, conditions, test results and medications to spot potentially harmful drug interactions. According to SafeMed, research trials showed medical decisions were altered for up to 1 in 10 patients based on the engine analysis, though some of these were for financial or lifestyle reasons rather than risk reduction. Information Week, 4 March 2008.

<sup>5</sup> IF PHRs were given greater privacy protections than institutional records, they could come to be the preferred venue for persons' most sensitive health data – a sort of Gresham's law of health information. "Sensitivity" tends to correlate with both the social stigma and the financial risk associated with a disease or condition. Data on the latter is potentially of greatest value for improving the cost-effectiveness of health care delivery.