

Primer: Data Protection and the Personal Health Record

Reid Cushman, PhD

Director of Operations, Medical Information Technology, UM-Miller School of Medicine
Project Health Design ELSI Team, University of Miami

Copyright and disclaimer: This content may be freely used for non-commercial educational purposes with appropriate attribution to the source (Project Health Design ELSI Team, University of Miami). This content is offered as educational material only. It is not intended as professional advice.

The new world of computing and communications

The rise in power (and fall in price) of personal computing devices, of electronic data storage,, and the ubiquitous data communications of the World Wide Web, permit personal management of data as never before. That includes the data type of interest here: personal health information embedded in Personal Health Records (PHRs).

Unfortunately, the legal requirements, professional norms and social customs of data protection are still oriented toward a world of institutional data repositories. Until these recent technological changes, only institutions had the means and motives for organized electronic data collection.

Means should be understood in both the technical and financial sense. Users of personal computers and the Web may take it for granted that computing and data communications have been “democratized” – i.e., put within the reach of essentially every one who can afford the associated devices and services. The unfortunate reality is that data protection (a.k.a., data security) remains a complex endeavor, beyond the reach of most persons. Moreover, institutions have not disappeared from the mix.

Personal vs. institutional “records”

The label “Personal Health Record” carries an etymological tension. In the oldest senses of the term (dating from the 1300s) “records” are official documents “committed to writing as authentic evidence of a matter ... evidence which is thus preserved, and may be appealed to in case of dispute.” ([Oxford English Dictionary](#))

It is not until the late 1800s that “record” evolves to its more modern meaning of “something that can be reproduced” (such as the sound on a phonograph or a photograph from a camera). And not until the late 1900s that it arrives at the abstract mapping of the computer age: “a number of related items of information which are handled as a unit.”

This is more than fodder for Scrabble discussions. Institutions are presumed to have the resources to assure the confidentiality, integrity and availability of their official records. There are sanctions for organizations, and sometimes for the persons who administer records of organizations, should they fail in that task. (See e.g., HIPAA’s [civil and criminal penalties](#) for mismanagement of health care records.)

What of individuals? There is relatively little law or social convention for what responsibilities fall on individuals who maintain the kinds of records once the province

solely of institutions – in the case of PHRs, a kind of record that until recently patients were sometimes not even allowed to see. (Only in 2003 did HIPAA establish at a national level the right of patients to examine their health records.)

Is the PHR best viewed as a complement to the official record – a nice thing to have, with greater or lesser value depending on the Personal Health Applications (PHA) it supports? Or is it a substitute for an official record – required in emergency situations (an electronic form of “medical alert bracelet”) and perhaps required even in routine ones because of the absence of inter-operable, inter-institutional electronic medical records (EMRs)? How much reliance can (or should) a health practitioner place on the data within a person’s PHR at a routine clinical encounter?

Whatever the legal, professional and social answers to these questions, there are technical constraints that limit what can be expected of the average individual. To understand those limits requires some discussion of the technical “platform” on which PHRs and PHAs are based, and some discussion of how the information security typologies derived from a world of organizational information collections apply.

Current platforms for PHRs and PHAs

Paper PHR It is worth remembering that the most common media for PHRs remains paper. (Unfortunately, it also remains common for health care organization’s authoritative health records.) Paper-based PHRs can provide a great deal of value simply and cheaply. Thanks to the ubiquitous photocopier, paper records are easy to reproduce. A list of allergies, medications and a summary of pertinent past medical history may be all that is needed in emergency situations, and provide the preponderance of information value in many non-emergency ones.

PC-based PHR Paper’s defects as a recording media are well understood. In particular, paper is hard to update. That problem can be eliminated by maintaining a “paper” PHR as a free-form text document stored on a personal computer (PC). Personal Health Applications installed on the PC can manipulate this data if it is taken from free-format text to structured storage. This may be the second most common form of PHR in place today.

Portable storage PHR PHRs are sometimes defined as “your health data on a stick.” The stick in this case is a “flash drive” (the name derives from the use of “flash memory” solid state memory chips). Flash drives are a perfect exemplar of today’s electronic data storage – small, portable, and very high capacity. Smartcard-based health records are a variation on this theme (chips embedded in a card form factor instead of a stick), which may be purely storage devices or include algorithmic capabilities to manipulate the data.

Backups for PHR Card and stick storage platforms can be easily lost or stolen (they are not just portable for the legitimate owner), and though resilient compared to a hard drive or floppy can also be damaged relatively easily. Encryption based on password or fingerprint can protect a portable storage device, but passwords can be lost (and fingerprints don’t always scan appropriately). (For more, see the Primer on Authentication of Identity.)

Thus, as with paper, the copy of data on a portable electronic PHR device should never be the only copy, at least if it is data that has any significant value or replacement cost. There must be backups. Who (or what) will keep them?

Internet storage PHR Since one may see a health care provider anywhere, particularly in an emergency, the backups must be accessible anywhere the data subject (a.k.a., patient) might be. The Internet (specifically the World Wide Web) is the only practical communications platform for this role.

Tools exist for remote communication to an individual's PC over the Web. The complexities of such tools tend to put them beyond the reach of the casual computer user, and the vulnerability of PCs makes it a risky platform in any case. It is thus unsurprising that the number of that institutional players offering (or planning to offer) Web-accessible repositories for PHRs, as well as applications for them, is growing fast (see Appendix A).

PHAs on top of PHRs Web-based Personal Health Application (PHA) tools can present PHR data in new and interesting ways. So could a PC, of course, but with the limitation of storage in a single location (if a desktop PC) or a moderately inconvenient portable one (if a laptop). In particular the use of Web 2.0 tools to create "personal health portals," embedded with personal health widgets/gadgets, provides the potential for customized sites that are both useful and compelling to use.

This brings the PHR full circle. It is "personal" in the sense of containing data related to that person, and perhaps also in the customized presentation of that information. But in this scenario it is no longer solely a personal record. Institutions are now part of the PHR mix, proving backup and value-adding applications, and so the legal and social constraints on organizational record holders gain relevance again.

The goals and methods of data protection

Information security specialists commonly refer to the "CIA," but they're usually not talking about the [Central Intelligence Agency](#) or the [Culinary Institute of America](#). Rather, CIA is an abbreviation for the widely used three-part benchmark for evaluation of information systems security: focusing on the three core goals of confidentiality, integrity and availability of information.

Confidentiality (a.k.a. privacy) Confidentiality refers to limiting information access and disclosure to authorized users of data – "the right people" – and preventing access by or disclosure to unauthorized ones – "the wrong people." Confidentiality is related to the broader concept of data privacy – limiting access to individuals' personal information. Data privacy is in turn just one piece of the privacy landscape, which includes limiting access to the physical self as well as data representations of it.

How is confidentiality protected technically? Authentication methods like user-IDs and passwords are one key method. (Likewise, newer authentication methods like token cards, similar to ATM cards, and biometrics like fingerprint scanning.) Authentication methods aim to uniquely identify users of data systems, and thus control access to the data systems' resources. Authentication is only one part of that, however. Access

control methods must translate authenticated identity into permitted and non-permitted activity rules, and then enforce those rules.

How is confidentiality protected legally? In the US, a range of laws and associated regulations, with abbreviations like [FERPA](#), [FSMA](#), and [HIPAA](#), set the legal terms of confidentiality. Unlike in European nations, where the approach to data protection is organized across sectors, the US reflects its Madisonian traditions with multiple, sector-specific restrictions at both the federal and state level. For any given type of data, there may be literally thousands of legal controls that apply.

Sorting out those thousands of rules occupies innumerable in-house privacy officers, security officers, lawyers and other professional staff of data-holding organizations. (It occupies and enriches a significant number of outside counsel and consulting firms too.) If you work for a data-holding organization you may have been “educated” on some of these requirements yourself, since workforce education is a standard requirement of confidentiality-focused laws and regulations.

Integrity Integrity refers to the trustworthiness of information resources. It includes the concept of “data integrity” – namely, that data have not been changed inappropriately, whether by accident or deliberately malign activity. It also includes “origin” or “source integrity” -- that is, that the data actually came from the person or entity you think it did, rather than an imposter.

Integrity can even include the notion that the person or entity in question entered the right information – that is, that the information reflected the actual circumstances (in statistics, this is the concept of “validity”) and that under the same circumstances would generate identical data (what statisticians call “reliability”). System designers are occupied by generating technical methods to keep humans from making data integrity errors, particularly for institutional EMR applications. Those technical provisions are reinforced by organizational policies and procedures that promote data accuracy and punish data inaccuracy.

On a more restrictive view, however, integrity of an information system includes only preservation without corruption of whatever was transmitted or entered into the system, right or wrong. That is, as a purely technical task. A variety of corruption-checking mechanisms can be used to detect wayward bits. Encryption methodologies, while generally viewed as mechanisms to protect confidentiality, do equally important work preserving data integrity.

Availability Availability refers, unsurprisingly, to the availability of information resources. An information system that is not available when needed is almost as bad as none at all. It may be much worse, depending on how reliant an organization has become on a functioning computer and communications infrastructure. A modern medical center has a near-total dependency on functioning information systems, particularly those that have moved to fully “paper-less” medical records.

Availability, like other aspects of security, may be affected by purely technical issues (e.g., a malfunctioning part of a computer or communications device), natural phenomena (e.g., wind or water), or human causes (accidental or deliberate). While the

relative risks associated with these categories depend on the particular context, the general rule is that humans are the weakest link.

Prevention vs. detection Security efforts to assure confidentiality, integrity and availability can be divided into those oriented to prevention and those focused on detection. The latter aims to rapidly discover and correct for lapses that could not be – or at least were not – prevented.

The balance between prevention and detection depends on the circumstances, and the available security technologies. For example, many homes have easily defeated door and window locks, but rely on a burglar alarm to detect (and signal for help after) intrusions through a compromised window or door. Information systems use a range of intrusion prevention methods, of which user-IDs and passwords are only one part. They also employ detection methods like audit trails to pick up suspicious activity that may signal an intrusion.

Security in context: organizational and personal

It is critical to remember that “appropriate: or “adequate” levels of confidentiality, integrity and availability depend on the context, just as does the appropriate balance between prevention and detection. The nature of the efforts that the information systems support; the natural, technical and human risks to those endeavors; governing legal, professional and customary standards – all of these condition how CIA standards are set in a particular situation.

The legal, professional and social norms of CIA have evolved in the context of institutional record-holders. The data-holding institution has a fiduciary responsibility to its stakeholders to protect the data under its control. The stakeholders include the data subject, of course, but also the institution’s own affiliates who rely on data for their work. In a health care context, for example, both patient and physician have an interest.

Legal protections for data subjects Health care has evolved from a world of solo practitioners to group- and institutionally-affiliated ones. Health care records have evolved from being the “property” of the sole practitioner to the “property” of the group or the institutional holder. US state laws, and after 2003 the federal regulations associated with HIPAA, define the legal relationship between institutional record holders and data subjects (a.k.a., patients) with respect to this particular kind of property.

What are those rights? Data subjects have a federal right under HIPAA to:

- to [inspect and obtain a copy](#) of their health records (except for psychotherapy notes which may be redacted);
- to [correct or amend](#) any errors in those records (or, at a minimum, put a statement of exception in the record for information with which they disagree);
- to receive an [accounting of any disclosures](#) of the records;
- to request [additional protections](#) for or [confidential communications](#) of particularly sensitive information in the records;

In addition, the data subject must:

- be given a [notice](#) of the institution's privacy practices on first contact, and periodically thereafter;
- sign a written [acknowledgement](#) of receipt of that notice;
- for organizations that choose such an option, also sign a [consent](#);
- sign an [authorization](#) prior to any “extra” uses and disclosures, such as [research](#) (institutions may not condition treatment or payment on an authorization);
- be given an [opportunity to agree or object](#) to other types of use or disclosure; and
- be provided with the names, offices and procedures for [complaints](#) about an institution's privacy practices (as well as the procedures for complaining to the federal Department of Health and Human Services).

Health care institutions covered by HIPAA must put in place data protection policies and procedures which give effect to these protections (defined under HIPAA's Security Rule).

Persons familiar with HIPAA understand that there's much less here than meets the eye. HIPAA regulations carve out broad exceptions that undermine the force of these rights. Nonetheless a world with HIPAA is probably better than the hodge-podge of state laws that preceded it.

Obligations of PHR holders Now consider a world of personal health records, where the data subject *is* the data holder. Legal-regulatory regimes that define relationships between data subject and institutional holder don't address this world, except in the circumstances where the institutional holder is the “backup.” Does it make sense to even speak of individual obligations in a PHR world? Isn't the data subject holder obligated only to him- or herself with respect to the PHR and the applications that derive from it?

In this world, there are still third-parties, the protection of whose interests is at least worth discussing. Personal health records may – and, to be complete, must – include data on family health history. The family members that are the subjects of that history have a clear confidentiality interest in the data. This interest only grows stronger as genetic information is integrated into personal health data. “History” becomes expressed not merely in narrative.

Integrity and availability issues also occur in this world, to the extent that others place reliance on the data within the PHR. The ability for the patient him/herself to update PHR data manually, as well to add “automated” data from personal sensors and devices, could allow PHRs to become a valued supplement to institutional health records. However, health practitioners cannot use the PHR to guide diagnoses or treatments without some assurance that the data are correct (integrity) or that it will be accessible when needed (availability).

It's true that each patient-practitioner dyad could negotiate its own rules about how to treat the PHR's information relative to that in the institutional EMR at hand. That seems a fairly burdensome arrangement, however, if it must be negotiated afresh at each encounter. But it may be an inevitable concomitant of any PHR. Indeed, one could say it is already inherent in a world where patients bring their lists of allergies, medications and past medical histories, even if such data is embedded only in the pressed fibers of a dead tree.

Conclusion

The presence of extensive third-party players in the “personal” health record space requires that legal-regulatory regimes give careful attention to the requirements on third-party behavior. HIPAA does not currently apply, since it reaches only to [“covered entities”](#) like health care providers and health information clearinghouses. Most state laws, in their current form, are inadequate to the task too.

Model legislation, to guide the states in the approach to the PHR/PHA world, could make for a considerable contribution.

Appendix A – PHR/PHA offerings in the current market

(Source :American Health Information Management Association)

Product Name	Format	Cost
AboutMyHealth	Internet Service	Free
CapMedPHR	Software Program	Purchase
Caregiver Alliance Web Services™	Internet Service	Purchase
CheckUp	Software Program	Purchase
Compiling Your Family Health History	Paper-based	Purchase
Dr. I-Net	Internet Service	Free
DrGlobe.com	Internet Service	Purchase
EMRy STICK	Software Program	Purchase
Follow Me	Internet Service	Purchase
Full Circle Registry	Internet Service	Purchase
GlobalPatientRecord	Internet Service	Purchase
Google Health	Internet Service	Free
Handymedical.com	Internet Service	Purchase
Health File	Software Program	Purchase
Health Minder	Software Program	Purchase
Health Profiler	Software Program	Purchase
Health Records Online	Internet Service	Purchase
Healthcare Passport	Paper-based	Purchase
HealtheTracks™	Paper-based/Internet Service	Purchase

HealthFolio	Software Program	Purchase
HealthFrame	Software Program	Purchase
Healthgram.com	Internet Service	Purchase
HealthString	Internet Service	Purchase
HealthTracer	Internet Service	Purchase
I.C.E. Alert™	Software Program	Purchase
ICER-2-Go	Software Program	Purchase
iHealthRecord	Internet Service	Free
InstaHelpCard	Software Program	Purchase
Interactive Patient™	Software Program	Purchase
iPHER	Software Program	Purchase
IQHealth	Internet Service	Purchase
I-trax	Internet Service	Purchase
iValley	Internet Service	Free
Jakoter Health Organizer	Paper-based	Purchase
K.I.S. Medical Record Solutions	Internet Service	Purchase
Laxor	Internet Service	Purchase
LifeLedger	Internet Service	Purchase
LifemastersOnline	Internet Service	Free
LifeSensor	Internet Service	Purchase
Lynxcare	Internet Service	Purchase
MedDataNet™	Internet Service	Purchase
Medefile	Internet Service	Purchase
Medical ID Card	Internet Service	Purchase
MedicAlert	Internet Service; Software Program	Purchase
MediCompass	Internet Service	Free
MediKeeper	Internet Service	Purchase
Med-InfoChip™	Software Program	Purchase
MedKey	Software Program	Purchase

MedNotice	Internet Service	Purchase
Merck Source	Paper-based	Free
My Family Health Portrait	Software Program	Free
My Health	Internet Service	Purchase
My MedicalCD	Software Program	Purchase
myHealthFolders	Internet Service	Free
MyLifeSaver	Internet Service	Purchase
MyMedicalRecords.com	Internet Service	Purchase
MyMediList	Internet Service	Free
MyMeds	Software program	Purchase
MyMedSafe	Internet Service	Purchase
MyNetRecord.com	Internet Service	Purchase
MyPHR.com	Paper-based	Free
MyPRO™ Medical-Health Records Organizer	Paper-based/Software Program	Purchase
NoMoreClipBoard.com	Internet Service	Purchase
Patient Power	Internet Service	Free/Purchase
PatienTrak	Internet Service	Purchase
People Chart	Paper-based/Software Program/Internet Service	Purchase
Personal MD	Internet Service	Purchase
Personal Medical Diary	Paper-based	Purchase
PHR4me	Internet Service	Purchase
ProfileMD	Software Program	Free
RelayHealth	Internet Service	Purchase
Securedmed	Internet Service	Purchase
So Tell Me...™ Medical Organizer	Paper-based	Purchase
Synchart	Software Program/Internet Service	Purchase
Telemedical.com	Internet Service	Free
The World Medical Card	Software Program	Purchase
TouchNetworks	Internet Service	Free

TravHealth	Internet Service	Purchase
VIA	Internet Service	Free
VitalChart	Internet Service	Purchase
WebMD Health Manager	Internet Service	Purchase
WorldMedcard	Internet Service	Free
Your Health Record	Internet Service	Purchase