Health Privacy: The Way We Live Now

Robert Gellman
Privacy and Information Policy Consultant
Washington, DC

Appeared in Free Congress Foundation, The Privacy Papers: Medical Privacy Revisited
(2002 Second Quarter)

A colleague called last week to discuss medical privacy. It was a personal matter. He recently had a medical procedure that he did not describe. He doesn't want me or anyone to know anything about his diagnosis or treatment. I didn't ask for details. For purpose of this article, I will identify my friend as Fred (not his real name).

Fred was contacted by a researcher who got his name from his physician. Fred was surprised at the call because he didn't give permission for his information to be disclosed to any researcher. It wasn't clear whether the researcher knew anything about Fred's condition. The study was designed to compare people who did and did not have the same condition so the physician may have only said that Fred qualified for the study. Fred couldn't ask more without disclosing the information that he was trying to keep secret.

Being a good citizen, Fred was genuinely interested in helping medical research. But protecting his privacy was a very high priority. He wanted to know if participating would risk disclosure of his secret. For Fred, the greatest risk is probably gossip. Could someone who knows him find out about his condition through a casual disclosure?

My answer was that any use of his information would increase the risk. However, you have to keep things in perspective. Disclosures of supposedly confidential medical information are routine today, and the researcher's proposed use was no worse than many others.

I began my description of health information usage with the physician's office. Presumably, everyone there knew (or had access to) the information about him. If Fred was also treated in a hospital, dozens or even hundreds of hospital workers might have had access to his records. This includes physicians, residents, nurses, ward clerks, orderlies, nutritionists, physical therapists, pharmacists, billing clerks, administrators, and others. Remember that hospitals are staffed 24 hours a day, so that several individuals share positions.

There is always a chance that one of these hundreds of hospital employees knew Fred, Fred's wife, or a relative, neighbor, or coworker of Fred. Some hospital staff are medical professionals subject to ethical restrictions, but not everyone is. Even with the clearest privacy rules, there is always the risk that someone will go home and say "Guess who I saw at the hospital today?"

Fred has other providers who know about his condition. A pharmacist, laboratory, or x-ray facility may know. These providers, like his doctor and hospital, have staff, lawyers,

accountants, and others who see patient records. If the provider is a nationwide or regional chain, then Fred's records might be accessed by computer in multiple locations.

Other institutions pay for care. Information flows from providers through clearinghouses to insurers, health plans, and HMOs. All of these organizations have staff, outside lawyers, accountants, computer service companies, and government regulators. Any of those individuals might have access to Fred's information. So might his employer, who paid for his insurance. If the employer's personnel department processed his claim, then people there already knew something about his condition. Even if they didn't process the claim, the employer might ask the insurer to disclose information for a review of health care costs. Workers' compensation claims involve additional institutions.

It was clear at this point that Fred did not like this state of affairs, but we had only just begun. I told him that if he suffered from a communicable disease (e.g., tuberculosis) or certain other conditions (e.g., cancer), the provider would be required to report the information to public health authorities. If he had a gunshot or knife wound, the police would be told. If he were the victim of abuse (e.g., child or elder abuse), that information would also be reportable. Some patient information ends up in permanent disease registries operated privately or by government agencies.

Then I turned to other government activities. Because Medicare paid for part of his care, the federal government had his records. If he knew a worker at the relevant agency, his secret might be disclosed. The federal Privacy Act of 1974 establishes protections against disclosure, but the value of those protections against gossip is limited. If the Medicare clerk who processed Fred's record is the second cousin of Fred's neighbor and recognized Fred's name or address, that clerk might casually tell the neighbor and the secret would be all over the neighborhood with no real chance to find the source. That clerk could just as easily work at the hospital, public health agency, pharmacy, or insurance company.

We aren't done with the government by any means. Federal and state agencies oversee the health care system. Should the office that licenses his doctor open an inquiry into the doctor's fitness, Fred's record could be relevant. The same would be true if the hospital was being reviewed for accreditation. Other governmental and private organizations engage in health planning, auditing, cost containment, outcomes evaluation, and fraud and abuse control. Any of these activities could lead to more disclosures to more people.

Federal, state, and local law enforcement agencies can access health records for different purposes. The authority of the police to obtain records varies, but in many cases, all they have to do is ask. Suppose that someone stole narcotics from the doctor's office on a day when Fred had an appointment. A list of patients might be given to the police. Fraud investigators usually have statutory or contractual rights to see records. If Fred's doctor became the target of a Medicare fraud investigation, the Inspector General at HHS might obtain the record and give it to federal investigators and prosecutors.

Fraud investigators are particularly worrisome. If they investigate Fred's doctor or hospital, they can see Fred's records along with thousands of others. If a provider improperly

coded a bill in an attempt to obtain more money for its services than it was entitled to, Fred's record could become evidence in a criminal or civil prosecution. Prosecutors could file a copy of Fred's entire medical record in court, and the record would be publicly available at the courthouse. This could happen although Fred had done nothing wrong. Even worse, if Fred's supposedly confidential record reveals some crime by Fred (e.g., drug abuse), the investigators could use that information against Fred.

I didn't think that he wanted to hear any more so I didn't tell Fred about other uses or about private litigation. A private litigant might be able to obtain his record if it was relevant to a lawsuit. Fred might not know if the record were subpoenaed and might not be able to object. If he did learn about a subpoena, he might have to hire a lawyer and go to court at significant expense to fight it.

We returned to Fred's original question about the researcher. He was being recruited for a multi-year, multi-university study. He wasn't offered a list of the universities or researchers involved in the study. It was possible that someone who knows him at a participating university might see his information. Did he know anyone who did health research, worked at a university computer center, or was a student at a university who might be working for the researcher on a work-study program as a data entry clerk? Any of those people might see his record and recognize his name. The more universities involved and the longer that the research continued, the greater the risk.

It is possible, and even likely, that his record would be de-identified at some point during the research to protect his identity, but the timing and protections from de-identification were uncertain. A security mistake could even put Fred's record on the Internet.

Even if Fred declined the invitation to participate in the research, the researchers might be able to see his records anyway without his knowledge or consent. An institutional review board (IRB) could approve researcher access and waive any requirement for Fred's consent. Many health care providers will disclose records with IRB approval. IRBs provide some independent review and control over researcher access. Fred observed that the IRB must have approved the researcher's plan to contact him without his consent and that seemed to be something different than just allowing a review of records. This made Fred wonder whether IRBs really offer much privacy protection to patients. I told him that some do a better job than others.

Fred had two questions. First, he wanted to know how many people had access to his "confidential" health information. The question cannot be answered with any precision. Assuming that his treatment included hospitalization and that a third party paid part of his bill, my best guess is somewhere between 1000 and 10,000 individuals. These people work at the dozens of organizations in Fred's community and across the country that routinely or occasionally have access to health records. The exact number depends on Fred's diagnosis, the value of his records to researchers, and random factors such as the chance of his record being involved in an audit or investigation. Fred was particularly concerned that most of those who might see his record are not health professionals subject to ethical rules.

I estimated that the strongest, practical, pro-privacy law that could pass in the current political environment might reduce the number by ten to twenty percent on the low side and by thirty to forty percent on the high side. Thus, even a strong privacy regime would still have his records accessible by perhaps 800 to 6000 people. Achieving that reduction would require a knock-down political fight.

Fred's second question was about the effect of the new health privacy rules that are about to become law under the Health Insurance Portability and Accountability Act (HIPAA). Fred knew that new privacy rules were coming and that politicians promised patients better control over the privacy of health records.

I told Fred that the new rules did not really change anything that I told him about the current health care system. HIPAA does not prohibit any disclosures routinely made today. The HIPAA privacy rules do not cover many institutions (e.g., researchers and law enforcement) that routinely obtain health records. The rules add some formality and new procedures, and they give him some new rights. Only two of the new rights are significant. First, the right to notice allows patients to learn how little protection health records have today. Second, patients also have a right of access to their own health records. HIPAA offers some other rights, but all are significantly limited or have broad loopholes.

As a society, we made a decision over the last several decades that concerns about medical confidentiality had to give way to concerns about public health, cost containment, quality and availability of care, and fraud and abuse. These worthy goals cannot be easily dismissed. Decisions were made in an era when no one paid much attention to privacy. Some activities that might have used anonymous health records were allowed to use identifiable records because no one insisted on anonymity.

To provide real privacy protections means changing many existing institutions so that they can function with less identifiable data. It also means fighting those institutions because none of them wants to change anything they do or to incur any cost or inconvenience in the interest of patient privacy. They all want to be left alone to carry out their activities – many perfectly reasonable and important – with as little disruption as possible. Indeed, many institutions want access to more identifiable health information, centralized patient databases, and new health identifiers so that they can control costs, improve care, and prevent the spread of disease.

The HIPAA privacy rules can be criticized for many reasons. Like most health privacy experts, I could offer dozens of major and minor objections. The truth is that we have already compromised health confidentiality in favor of other important (and sometimes unimportant) concerns. HIPAA mostly reflects the compromises we have already made. Revisiting those decisions would not be easy substantively or politically. It is easy, however, to stand on a soapbox, scream about the sanctity of health records, and demand better protections.

When our conversation was over, Fred went away unhappy. He said that he was troubled about the absence of privacy protections that he thought existed. He was mad about the essential dishonesty of the public debate over health privacy. He was conflicted over beneficial uses of

health records that nevertheless undermine his privacy. He was confused about how to fix the problem, especially in an environment where politicians make the decisions and mammoth health care institutions have lots of influence.

Fred is a pretty smart guy.