Socialized medicine + centralized database = distributed risk

By Tamara Wilhite

There are a number of proposals being brought forth to improve our currently chaotic medical services system. One of the greatest problems for care providers in an emergency situation is lack of access to a patient's inclusive medical records. Right now, every physician or specialist's office, hospital and Emergency Room may have its own records for a patient. Every time a patient visits a new practitioner, they must submit a request for the prior medical office to send the records to the new office. If patients are lucky, the old office sends an electronic file to the new doctor, and both are merged into a complete history. Typically a portfolio of paperwork – from patient history charts to test results to HIPAA permission forms – is mailed or faxed to the new office and appended to medical records the patient has already signed. The only place which contains all of a patient's medical data is the insurer. Medical insurer's records contain at the very least the date the patient visited, what the diagnosis was, and the reimbursement code assigned by the doctor to the patient's case which determines how the insurance claim will be processed and paid.

There is no centralized or easily searchable database containing every individual's medical records.

Unfamiliar or not, patient records are difficult for doctors to wade through during even routine visits. During an emergency, missing information in such a situation can be dangerous. The lack of information from other doctors can make the difference between life and death.

A few real world examples: A patient has a primary care physician. Then, due to a Friday night illness, sees a doctor at an emergency care center. That doctor prescribes medication based upon their assessment of the present condition, which the patient picks up at the pharmacy before going home. Then on Sunday, the patient becomes severely ill before falling unconscious. At the Emergency Room, the patient's primary care doctor is notified. However, the primary care doctor neither knows what diagnosis had been given the prior day nor the prescribed medications. The patient is not in a condition to share medical information, and the Emergency Room doctors may make incorrect decisions based upon current symptoms, instead of knowing the actual diagnosis and that the patient's condition has actually worsened.

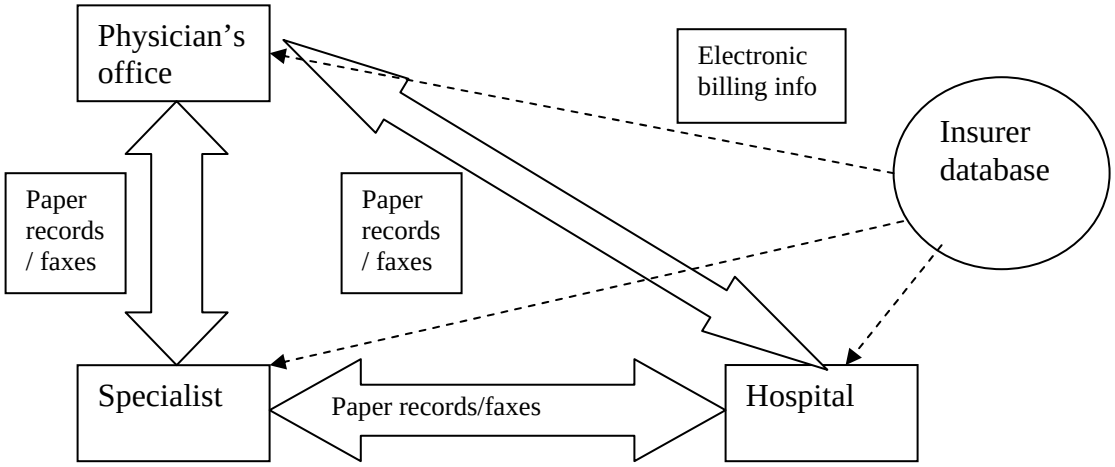
Another common occurrence is when a patient sees multiple specialists for multiple conditions. A dermatologist may prescribe Retina A or oral steroids. The Obstetrician/Gynecologist may prescribe hormones. The patient may take ~~herbs~~ herbal supplements from a chiropractor. If the patient visits a primary care doctor for a routine illness, he or she may forget to tell their doctor about a drug they are taking from another physician. Or, as is often the case, they may not mention topical medications or vitamins and herbal supplements because they are not considered "medications" by the patient. The lack of shared information between medical service providers increases the risk~~s~~ of

the primary care physician prescribing drugs that conflict with what the patient has already taken.

Another situation where cross-communication between physicians would be of benefit is patients who go in for diagnostic testing and never return to get the results. Many HIV and Hepatitis C tests are performed annually, with patients never returning for the results. It is a public health concern that these patients do not know that they are infected. As much of a patient's medical record is updated with information they personally provide, if the patient doesn't know they are infected, neither does their physician. If medical records were held in a publicly accessible location, their doctor or anyone else who treats them could inform them of the test results upon their next visit. This in turn reduces the patient's risk of exposing others to these deadly diseases, as well as ensures treatment is begun as soon as possible.

(continued)

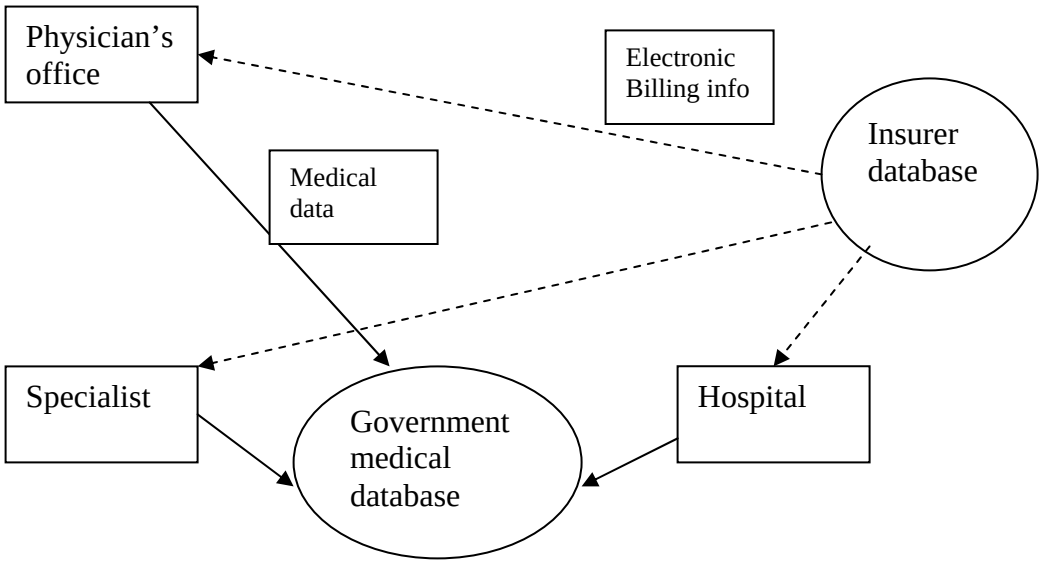
As it is today:



Pros:	Cons:
Information is kept only by the physicians and only shared when patients agree to it	Physicians don't have easy access to other practitioners' records, even when patients agree to share the information
Information is kept in multiple places, reducing the risk of potential loss	Redundant paperwork must be filled out by patients
Physicians have easy access to their own records	Delays in doctors sharing information with each other, if at all
The government cannot access information unless the medical claims are processed by Medicare / Medicaid / Veterans Administration	There is no centralized record of disease outbreaks or infected individuals unless the CDC requests and then correlates the data
If one physician has errors in your records, those errors are not propagated unless the incorrect data is forwarded to another–physician	Finding errors in your medical data means reviewing each doctor's records individually If an error is found within a medical record, the patient must review each physician's records individually for errors
Safety by redundancy - If one physician loses your records, the others still have their records	It would be difficult to accurately track which physicians have data on a particular patient

There are proposals to take everyone's electronic data and place it in a central government data repository. That system would look a little like this:

Currently proposed central database:



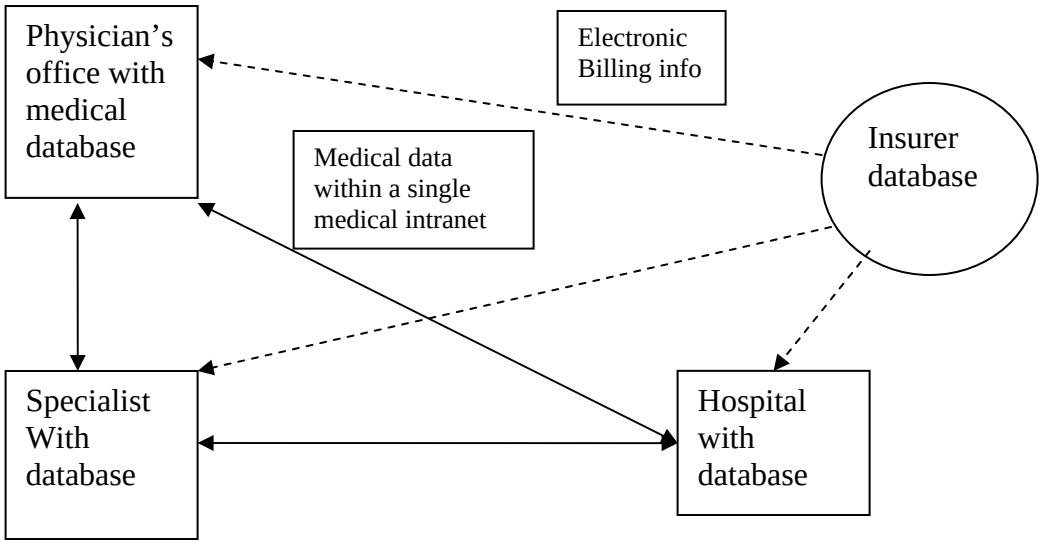
All of our medical information would hence be within a central government database, with hospitals and doctors uploading and downloading our medical data to this centralized system.

Pros:	Cons:
Information is easily accessible to physicians and medical professionals with access to the central government database	No privacy; any doctor/bureaucrat/hacker who can get in can see your medical information With multiple individuals in the private and public sector having access to the information, security and privacy are of increased concern.
Information is kept in one place, eliminating redundancy	The existence of a single database creates a risk – any downtime of the database due reasons such as equipment failure or the malicious actions of a "hacker" decreases the ability to provide care when information is not available.
Physicians have easy access to all patient records	If there is an error in your medical records, all physicians are affected by the same error

If there is an error in your file, it only has to be corrected in that one location	Try getting permission to see your medical records from the government; it's about as hard as getting social security records fixed or clearing up identity theft – i.e., NOT EASY In comparison with current centralized records systems in place, such as Social Security records, it may decrease accessibility of personal medical records to individuals
If one physician or office loses your records locally, it is still in the Federal system	If the central database loses your data, the data may be permanently lost.
There would only be one data format used for all records, eliminating the complexity in the current system which is a mix of paper records and electronic records in multiple formats, making it difficult for medical offices and hospitals to share data.	A massive effort would be required to convert data to a single format; if the data is corrupted when uploaded to the government system, the issue may not be found until it the originals are lost

(continued)

A better proposal:



All of our medical information would hence be within a database at each medical provider's office, accessible through a central INTRANET, with hospitals and physicians uploading and downloading our medical data to their own databases but accessible through a centralized and searchable medical record intranet.

Pros:	Cons:
Information is easily accessible to physicians and medical professionals with access to the central medical intranet	Privacy is again a concern as protected health information is accessible by more individuals
Information is kept in a known location, and is centrally accessible ;local accessibility to data possible even in equipment/software failure	The entire medical system could possibly be brought to its knees by one malicious person shutting down the network. Equipment or software failure could limit accessibility
Physicians have easy access to all patient records	If the network connection is down, physicians would not have access to a new patient's records (though this is true with the current system and any proposed replacement)
There is a centralized record of disease outbreaks or infected individuals, increasing the efficiency of epidemiology analysis	Privacy is again a concern as protected health information is accessible by more individuals; the possibility of information leaks – deliberate or not – becomes a greater concern.

With local databases sharing data, the redundancy provides a measure of protection. If your blood type is changed in one database, the other databases may not be touched; this mismatch would be a glaring red flag to be researched – and no other proposal has this type of protection.	The errors must still be tracked down and individually corrected. Fixing errors can time consuming.
If one doctor loses your records locally, other records are still in the network	If the central database loses your primary ID code (how you are identified) or if your ID is deleted, no one may be able to tie your records to you, making it as bad as not having your records in an emergency. Fortunately, a federated medical intranet could be re-synched between your ID and your records, once the missing identifier is correlated to your records again.
Each doctor could store their records in their own format, eliminating the risk of typographical errors when they entered data to a federal system	Conversion of data from one format to another used by different facilities still poses a risk of corrupting the data at the time it is needed; fortunately, the original information is still at is original database, and could be transferred by another method (fax/e-mail) if the network data transfer was not successful.

This medical data intranet could be privately run and maintained, keeping bureaucracy to a minimum while improving service (data quality and up time) due to free market principals. Multiple medical database intranets could function much like our credit bureaus do today, though with better security and fewer errors. Many of the problems that the credit bureaus create is due to lack of accountability to the data generators (banks, credit card issuers). If there is an error on your credit report, you dispute it with the credit reporting agency. But the original error may still exist in the original system and may still show on your report – and you often cannot get the information or permission to get the error corrected at the source. My proposal keeps that data tracking and accessibility to correct in place.

Furthermore, credit bureaus maintain a central database of their own, usually sharing data between the three of them. Errors on one may appear on all three. A medical data intranet may share data, but should not propagate errors. And the redundancy of data within the medical intranet would make errors pop out far more easily than if 2 out of 3 credit bureaus list a duplicate mortgage. Multiple medical intranets in private hands act as a strong counterbalance to the human error that can generate false data and mix up records. Competition may also act as a driving force for improved security and better software to support the application, as had already occurred for the Internet.

In this proposed system, there would be more checks and balances and the opportunity for the patient to catch and correct errors than exists in current government centralized databases. One real life example is the “No Fly” list. How many stories are there of Senators and babies who get denied access to flights? Now imagine how much work it is to get your name off of it.

My personal experience involved a medical record mix up in college. My HMO saw two individuals with similar names, the same birth year, attending the same college, and close by addresses. Thus “Tammy Britain” had her medical records merged with mine, “Tamara Britain” at the time.

I learned about this after going in for a renewal of a prescription and receiving a letter in the mail a week later for a very high cholesterol test. When I called the HMO, they stated it was just an error and that it would be corrected, and that I should not read test results intended for other individuals. I continued receiving test results for someone with high cholesterol, recommendations to lose as much weight as I weighed at the time, and a wide litany of issues. At the same time, I did not receive medical test results in a timely fashion when I went in for my own blood work.

After a dozen calls to a dozen different departments within the HMO’s company, I received the address for their records department. One individual had decided that two individuals were one, and that our records were merged. Untangling them proved difficult, because I could not state the other person’s address or social security number to verify that I was one of two; all requests were rebuffed as either a false record access attempt or insufficient verification (my address but incorrect SSN).

A physical visit to their records office in a nearby metro area was necessary to actually begin resolving the mistake. I took hard copies of some prior medical records indicating my prior plan membership number along with my membership ID card. A driver’s license and social security card and passport proved I was me, if not the “me” in their records. It required several demands in person with a refusal to leave to have the portfolio folder with my medical records produced. Within an hour, I was able to separate my paper records from that of Tammy Britain. I was informed that our records would be separated in their database per the new file, and thus the issue was resolved.

When I had my first child several years later, I received a drug to which I had a severe reaction. The doula (an individual certified to provide support and coaching during birth), who was also a personal friend, was able to rectify the issue. She asked to see my medical records to make sure all known allergies and conditions were noted in the records. Most information was correct, though that particular medicine was not listed as something I was not to be given due to family medical history. Whether not noted from prior procedures or lost, we didn’t know. This reaction led to a careful review of all medical records present by the doula. It was almost all correct. However, my blood type was listed as “O positive”. It is actually A positive.

When we were home with my daughter, I pulled copies of medical records and prior blood test results. The blood type error turned out to have been made ten years prior. Because I did not know my blood type at the time, I had never thought the information was wrong.

Fortunately, type O blood is not a medical hazard for someone who is type A. In reverse, the error is fatal. One data field not corrected, due to a minor medical record error many

years prior, had propagated onward through years of shared records. The error had only been caught because of a medical crisis and someone who happened to actually know the right answer.

In the current free market system, there are drivers that exist that could encourage individuals to utilize centralized government medical database in a malicious manner. There is great financial interest in "leaking" to the media private information of celebrities and public figures. To prevent this type of behavior some preventative measures would need to be in place. In addition, the vulnerability of a singular database to hackers continues to be a concern. The private medical intranet model would result in greater accountability for the leakers and hackers and far more traceability via access logs than a singular and much larger system may be able to provide

In 2008, an employee at UCLA Medical Center perused medical records for celebrities such as Maria Shriver, Farrah Fawcett, and George Clooney. Farrah Fawcett's records were actually sold to "*The National Enquirer"*. In January 2008, half a dozen employees were terminated for snooping in Britney Spears' medical records. If one employee at one facility having access to medical records is such a risk, multiply that risk of potential violation of privacy by millions of government officials and hundreds of millions of citizens and an infinite number of human reasons to look where one should not and possibly forward, copy or distribute such sensitive information. Then the possibilities of what can happen only expand as fast as access to the information.

One question that arises is: who owns this medical intranet? Not the government; that defeats the whole intent of accountability and consumer choice. It should not be insurers; the medical intranet's biggest benefit is portability of records (by not requiring them to be moved at all) by being outside of insurer control. Medical professionals may own their own database, but they cannot own our medical data. Otherwise, you may see the profit motive of being charged to make you records available to the medical intranet so that other providers can take care of you.

I propose that the medical intranet be owned and run by private companies, as the credit bureaus are of today. Of course, it will have to provide customer service as if our lives depend on it – because they do.