To Share or Not to Share: Ethical Acquisition and Use of Medical Data

Kate Fultz Hollis, MS
Oregon Health & Sciences University, Portland, OR

Abstract

The Health Information Technology for Economic and Clinical Health (HITECH) Act proposes the meaningful use of interoperable electronic health records throughout the United States health care delivery system as a critical national goal. As we have moved from medical records on paper to interoperable electronic health records, the rapid and easy sharing of medical data through the Internet makes medical data insecure. Electronic data is easy to share but many steps to ensure security of the data need to be taken. Beyond medical data security, we need to ethically acquire, use and manage data so that all people involved with the data from producer to data manager are recognized and respected. This paper advocates that sharing medical data can be ethically the right choice for everyone in health care if data sharing guidelines are available for people to use, modify and strengthen for specific purposes.

Introduction

In news sources and academic journals, we read terms like "big data," "medical data warehousing," and "data mining," and some of us could wonder what the actual data might be, who uses the data, or who owns that data. As medical informatics professionals, we should be able to describe the technical details of the data we use: coded information and text data from medical records and large database repositories in medical centers and clinics. From the patient's perspective, patients are concerned about how their own medical data can be used to improve their care but also if other data is available to help the health care team diagnose and treat patients. Many people are not sure what it means to have medical data shared between medical centers or between doctors in different clinics. Is this data safely shared? The Office of the National Coordinator for Health Information Technology (ONC) reported in 2015 that "(f)indings from national surveys conducted by ONC in 2012 and 2013 show that the privacy and security of medical records are significant and important concerns for individuals nationwide. About 7 in 10 individuals express concerns about privacy and security although less than one in 10 individuals have withheld information from their providers due to these concerns."[1] However, the same report concludes that "(e)vidence from this survey suggests that increased adoption of electronic health records (EHRs) is not associated with individuals' privacy and security concerns."[1]

Individuals want their data to be secure but they may also want their data available for many to use. Can we be sure that shared medical data is secure but that the data can be easily shared by appropriate individuals and institutions? It is hard to know what is the right way to handle the data and who really owns the data. Cheung, Martin and Asa addressed legal ownership of tissue samples in Canada and the US.[2] They noted that medical information can be blocked from use due to institutional ownership. Many individuals would want their healthcare data shared among people who provide their health care and perhaps some would want their data shared for medical research. However, the Health Insurance Portability and Accountability Act (HIPAA) restrictions allow patients to easily decline the use of their medical data for research and a conflict exists between those who want as much data as possible and those who want data restricted. Ness, in a 2007 survey, noted many problems conducting research due to HIPAA restrictions; however, he also concluded that "this survey did not address whether the effects (of research) reported may reflect the wishes that now can be expressed by better informed participants about the use of their health information and thus are the intended and laudable goals of the Privacy Rule."[3] Collins and Varmus wrote that "'Precision medicine' will also pioneer new models for doing science that emphasize engaged participants and open, responsible data sharing."[4] However, data needs to be appropriately secured from illicit use and, unfortunately, the ability to ensure data security is not always successful. This paper presents some recent problems regarding medical data sharing and the need for better and updated guides for ethical stewardship of shared data.

Big Data

How can we best define "Big Data" in medicine and health care? Medical Subject Headings (MeSH) from the National Center for Biotechnology Information does not have the exact term, and so we will use the MeSH term of data mining: "(u)se of sophisticated analysis tools to sort through, organize, examine, and combine large sets of information."[5] A clinician would be interested in finding information from large datasets about a difficult case the clinician is trying to treat; a patient would be interested in knowing how many people have the same disease the patient does and if these people get better from particular treatments. Essentially, is there a way all of us can be healthier if statistically the data we use leads to better disease treatments? Is all the data we need available for us and if not, why not? In *Lancet* in 2011, Boulton comments about data sharing, and he emphasizes the mixed (good and bad) record biomedical scientists have in data sharing and transparency. His notes are particularly interesting regarding the ethical use of data.[6] Boulton outlines some of the problems to be addressed regarding data sharing, and specifically, problems with open data, including:

> **Whose data?**
> Should open release only apply to those in receipt of grants from or employed by public funds? What about data from clinical trials, or data from safety analyses by private companies used to inform decisions of legitimate public interest (e.g., Deep Water Horizon and Fukushima)?
>
> **Confidentiality, privacy, security, and intellectual property**
> How should we cope with the need for confidentiality, anonymization, and data security? How would intellectual property rights be protected? How should we balance personal privacy against wider public benefit?[6]

Boulton mentions many data sources, such as unpublished clinical trial data, that could be very useful to researchers but are generally not easily available. Likewise, Drazen reports that unpublished data could help answer significant research questions.[7] Scientists know, and the public usually does not, that many clinical trials are completed with good datasets that are not published and there are datasets that remain at an institution never to be found. Drazen says, "There are many hurdles ahead to an effective data-sharing culture. We need to modify trial registries to hold additional information. We need to gather and store our data carefully so that they can be understood and shared by others. Ideally, a series of third-party data warehouses will spring up to facilitate data sharing; we need to be sure that these warehouses can hold the data securely while parceling it out to qualified parties."[7]

As much as we want standardized and de-identified open data, the reality is that many producers of different data sources are not following the same standards for data format or the proper benchmarks to de-identify subjects in a research study. We need to be careful about how personal health information is disclosed only to appropriate parties doing the research.[8] McGuire et al. note that the inclusion of genomic test information in EHRs brings about large databases of genetic information that could be "mined for individual identification purposes."[9] Sweeney et al. have shown that large sets of publically available data can be used to identify de-identified data like that in health databases for research.[10]

However, Hunter et al. attempted to present methods to de-identify data that would help the scientist to share data, the clinician to use that data, and ultimately, the patient to benefit from the data in terms of new treatments. In a paper with the ethical standards strongly considered, they said:

> Our proposal is based on four balancing ethical principles: beneficence, justice, trust, and privacy. Beneficence entails the duty of researchers to act on behalf of the study participants' welfare by maximizing the benefits and minimizing the harms of research. In the case of this proposal, the benefit is a meaningful improvement in health. Although the benefit is limited to the small number of people who participate in research and have an actionable result materialize, the number of people affected may grow with advances in proteomics and genomics research. There can conceivably be negative consequences to providing actionable results to research participants, including anxiety and the costs of further evaluation; these would be disclosed in the consent process. As with any other aspect of consent, a participant could opt out of the potential to be informed of actionable results at any time.[11]

We can share secure data if we can present good methods to de-identify data appropriately to everyone involved in the research process (including the patient). Hunter's emphasis on opting out for the patient should be considered in any step to share the patient data. While Ness stressed that patient refusal to share medical data hampers medical research, Hunter et al. propose a step-by-step process to opt out at any time so that at no time does the patient feel trapped by a decision made at the beginning of a study.

From another perspective, it might be better to consider personal medical data as a gift to give for research. Taylor and Mandl suggest that if we enable data "donation" by individuals, the impediments of obtaining consent to reuse data might lessen and there would be active involvement by patients to allow data to be freely shared. They state in their 2015 policy paper that "in contrast to charitable financial donations where template legal arrangements abound, data donation faces a vacuum. We believe that, if conditions were reasonably structured and well-known, both 'information altruists' and disease-specific, self-assembling patient groups will donate data to speed social and direct benefit through innovation and research."[12] Once data is available, we would also need to make sure it is safe to use for anyone with a good purpose for the data. An institution has an obligation to take care of donated data as institutions should provide stewardship of donors and of the items received from donors. But what if the institution treated the data more importantly than they treated the donor? Cases such as the Markingson case described below have appeared where those who use patient data might feel that the data is more important than the patient. Even if data was donated, data ownership becomes a difficult ethical problem for the researcher, clinician, and the institution.

Data Ownership

If we want to share data we have collected from a patient or a tissue bank, do we have permission to share that data? Organizations have an Institutional Review Board (IRB) to process consent agreements with human subjects for research and approve the proper security and data sharing process for a research experiment. This process includes institutional definition and adherence to data sharing policies, including security of the data.[13] However, the 2004 Markingson case at the University of Minnesota is an example where the university's IRB did not pay enough attention to the care of patients in a clinical trial for anti-psychotic medications. The acquisition of data was more important than the patients and in fact, one patient committed suicide while in a clinical trial that was testing three drugs.[14] McCarthy in the *British Medical Journal* writes:

> The report found that the reviews of the case by state, federal, and university bodies were often superficial or compromised by conflicts of interest. The university's institutional review board, for example, did not review medical records, did not review information about Markingson's suicide, and did not seek information from anyone other than Stephen Olson (the study principal investigator), the report found. The Minnesota Board of Medical Practice review was done by an expert consultant who had been on the university's institutional review board when it approved the CAFÉ study, had been the chair of the institutional review board committee that had reviewed Markingson's death, and had received more than $83 000 (£56 000; €76 000) in payments from AstraZeneca in 2006 alone. A Food and Drug Administration review found no evidence of misconduct, the report noted, but that review "never discussed the potential coerciveness of obtaining consent from an individual under a stay of commitment."[14]

This case was particularly difficult as Dan Markingson was given a choice of being in the trial or being committed to a state psychiatric hospital so as a patient he was not given a choice about the experiment and the IRB seemed not to follow any ethical guidelines for the autonomy and non-malfeasance of patients. How would the data from this trial be collected ethically if there were severe consequences for the patient in regards to data collection?

The Markingson case is a severe example where the research study did not take proper care of the patient. The principal investigator (PI) of the study, Olson, was under pressure by Astra Zeneca to keep Markingson in the study and in the State of Minnesota's case against the university, the report stresses "(u)niversity officials' unwillingness to acknowledge and address this wider range of ethical problems is troubling. Rather than acknowledge the concerns, university officials have dismissed them and essentially said there is nothing to talk about."[14] In addition to their disrespect of the patient, the PI and the company valued data about the drugs more than that the data that belongs to this patient should be treated with respect and used to treat the patient better. As Hunter et al. had noted, researchers must seek to maximize the benefits of the research for the patient and minimize the harm.[11] The researchers and the university in the Markingson case certainly did not follow the ethical principle noted by Hunter.

Ethical principles for the data are important and data interoperability should be appropriately done. Interoperability of health care records is difficult when two different computer systems cannot exchange data for a variety of technical reasons. We fortunately have many organizations and government agencies working to make data interoperable (e.g., the ONC and "Structured Data Capture"[15]) but there are still instances where doctors keep the electronic data of their patients at one clinic and the excuse can be that the data is not transferable whereas the data might be non transferable only because the doctor or clinic doesn't want to share the data. In *Modern Healthcare*, Goozner wrote, "Most Americans who receive care at more than one location still don't have their 'complete' record in front of their attending physician. Heck, most providers can't or won't even send their patients' electronic records across town, much less to a neighboring state or across the country."[16]

John Creswell, in the *New York Times,* also covered this issue of doctors being unable to connect to other computer systems and in some cases, the electronic health record companies were to blame. There is no evidence that any vendor cannot technically share data with another vendor but "Epic and its enigmatic founder, Judith R. Faulkner, are being denounced by those who say its empire has been built with towering walls, deliberately built not to share patient information with competing systems. Almost 18 months after an Epic system was installed at UnityPoint Health-St. Luke's Hospital in Sioux City, Iowa, physicians there still cannot transmit a patient care document to doctors two miles south at Mercy Medical Center, which uses a system made by another major player in the field, the Cerner Corporation."[17] Why is data not being shared? Is data so valuable that we need to place monetary value on the data?

Data Blocking

In May 2015, Robert Pear reported in the *New York Times* that "some tech companies, hospitals and laboratories are intentionally blocking the electronic exchange of health information because they fear that they will lose business if they share information on patients with competing providers, administration officials said. In addition, officials said, some sellers of health information technology try to 'lock in' customers by making it difficult for them to switch to competing vendors."[18] Big data are a big asset for hospitals and for companies interested in keeping customers and developing better health care products. But is this electronic record data technically their data to block? There is plenty of concern from the ONC about information blocking from EHR vendors and hospitals, so much so that a report about information blocking was published by the ONC in May 2015.[19]

Information blocking might be legal and a good business strategy. Certainly companies have proprietary information that is their property that they protect from other companies in order to increase their profits and protect their investment in, for example, the company EHR use at medical centers. But is the information they collect from EHRs for clinical trials or the information the EHR vendor collects technically information that they own and therefore should be able to keep for their own uses? The federal government who provided the money for interoperability is certainly not happy that companies or hospitals would block information to the public, as the Affordable Care Act (ACA) stipulated that information needs to be exchanged between all care givers. The ONC's 38-page report is interesting for the details it presents about how a hospital or a company might block medical data and also for the lack of data about who or what might be currently blocking data. John Halamka had a discussion with Health Leaders Media (HLM) about information blocking, and here is part of the transcript:

> HLM: ONC says it's gotten 60 reports of information blocking. Might it be happening in a less obvious way?
>
> Halamka: I am guy who has no agenda. I am not dogmatic. I will evaluate any evidence that it put front of me. Maybe there's a niche vendor that's doing it, but I've never found a mainstream vendor who is going to go against the wishes of its customers to exchange data.
>
> HLM: One complaint is not that vendors refuse to share data, but that they are charging a lot to do it.
>
> Halamka: The question is, what's a lot of money and what is the work involved? If people complain that 'my lab interface was $5,000,' well, if it's a novel lab interface that's never been done before, it is a substantial amount of work to map all the lab tests. It actually takes me about 16 weeks to produce a lab interface. So I don't think $5,000 is unreasonable. Others may. Again, look at the data. Let's see what people want done and what's being charged for it.[20]

We could probably imagine that information blocking happens as there have been anonymous complaints about blocks. The ONC's report[19] does not specify the individuals or the organizations but the report includes some rather specific examples of data blocking that would be hard to say were made up for the report. The ONC presents guidelines for governance rules that would foster shared protected health information and open exchange of medical information. Halamka is right that for some companies or health care institutions, the money for creating an interface that works better and can help people and organizations share health care information easily might need to be compensated for the work put into the mobile application or the computer system. However, if extravagant costs become unsustainable for patients or hospitals, the value from information sharing would be diminished. In this case, we might want to invest in better tools to share secure data rather than allow companies and hospitals to block data.

Halamka has a point about not finding a mainstream vendor to go against the wishes of the customers to exchange data but if the customers include patients and their health care providers sometimes an individual wish does not have priority. In 2001, Ball noted the rise of the patient as consumer and one that is powerful with regards to becoming connected with the physician and the health care enterprise. "Indeed, new tools will allow both physicians and consumers to operate differently and think differently. They will achieve a new level of knowledge and connectivity, and the inefficiencies that bar them from fast access to crucial clinical answers will largely disappear."[21] In terms of whether we are there yet with fast access is hard to say; however, it does not make any sense to block information that we really need for better healthcare.

But there are problems with data sharing in terms of legitimate data transfer: is data owned by the patient, the researcher, the institution that supports research, the clinic that maintains the medical record, or not owned by any person or entity? There are issues of legal ownership of data: the health care clinic is the steward for the data so the clinic might own the data. The patient pays (or pays insurance) to have a test done, so doesn't that patient own the data from that test? Questions about who funded the data makes it hard to pinpoint who owns the data.

The University of California, San Diego (UCSD) and the University of Southern California (USC) went to court against each other to decide where a study's data belonged.[22] Paul Aisen from UCSD took the data from his work on the Alzheimer's Disease Cooperative Study (ADCS) at UCSD and brought the data with him to USC. UCSD contested Aisen taking the data to USC and UCSD was "was especially aggrieved by what it regarded as the secretive nature of USC's recruitment of Dr. Aisen. 'USC engaged in months of negotiations with Dr. Aisen as if the ADCS were Dr. Aisen's personal property, without any attempt to communicate with UC-San Diego in advance,' said Gary S. Firestein, associate vice chancellor and dean of translational medicine at UC-San Diego. USC, in turn, said that it does not seek the entire ADCS from UC-San Diego, and would be happy to discuss a resolution without involving the courts."[23] This case will probably continue in court but there did not seem to be an ethical transfer of data from one institution to another at least in the opinion of the institution that lost the data. If there were guidelines about where the data belongs and who owns the data, it might be easier for either institution to make their case that the data belongs to them. NIH maintains that grant recipients are institutions and that the institution generally owns the rights to the data.[24] However, so many different ways to interpret who owns this data make the case complicated.

Ethical Guidelines for Data Sharing

We have discussed instances of big data, data ownership and data blocking. What would be an ideal situation for sharing medical data that would benefit everyone involved in the medical enterprise? There should be more guidelines about data sharing but the ethical statements about "Big Data" sharing appear scarce. Table 1 shows some of the ethical statements available from the federal government and one association about data sharing. However, if one is looking for specific details about how data might be shared with everyone involved in the data process, it might be hard to find guidelines about that. This table is not an exhaustive list of policies on medical data sharing and does not include individual institutional policies. The guidelines listed in the table are the relevant statements on data sharing made by a few entities. Not all of the items in the table are listed as "statements" about data sharing ethics but all contain some information about how data should be handled appropriately.

Table 1. Ethical guidelines

Organization	Data Guideline	Date Updated
Final NIH Statement on Sharing Research Data[24]	(T)he rights and privacy of people who participate in NIH-sponsored research must be protected at all times. Thus, data intended for broader use should be free of identifiers that would permit linkages to individual research participants and variables that could lead to deductive disclosure of the identity of individual subjects. When data sharing is limited, applicants should explain such limitations in their data sharing plans.	2003

Organization	Data Guideline	Date Updated
American Society of Human Genetics Code of Ethics[25]	Members protect the privacy of the individual, especially in light of concerns over possible discrimination and confidentiality of medical information. ***Confidentiality*** Respect the confidential nature of all information entrusted to them. Disclosing personal health information with proper and specific authority through the consent of the individual or where there is a legal, ethical or professional right or duty to disclose. ***Storage and security*** Maintain confidentiality in creating, storing, accessing, transferring, and disposing of personal health information.	2006
NIH Genomic Data Sharing (GDS)[26]	For research that falls within the scope of the GDS Policy, submitting institutions, through their Institutional Review Boards (IRBs), privacy boards, or equivalent bodies, are to review the informed consent materials to determine whether it is appropriate for data to be shared for secondary research use. Specific considerations may vary with the type of study and whether the data are obtained through prospective or retrospective data collections. NIH provides additional information on issues related to the respect for research participant interests in its Points to Consider for IRBs and Institutions in their Review of Data Submission Plans for Institutional Certifications.	2014

On September 8, 2015, the Federal Register proposed an update to the "Federal Policy for the Protection of Human Subjects."[27] The details regarding the care of human subjects in research and in particular the care of human subject data for research need close examination by researchers and patients. Several times during the comments section of the proposed rule, the notion of ethical regard for subjects and data are highlighted. "An increase in trust and partnership is likely to increase participation rates in research; using individuals' samples and data without permission will hinder true partnership. Better communication and community engagement with patients, particularly in geographic areas and for population subgroups where consent rates are lower than average, should be a priority for the research community."[27]

In an ideal world, researchers would know where to find all the data for their study and would be able to track data from when they send the data to a recipient and when they receive data. But as we know from several instances of data breaches and when data ends up in an unsecured place, we have difficulty keeping account of shared data. More care in defining what data needs to be secured and how it should be secured is important for the research enterprise. Some detailed outlines of how to protect human subject data are proposed in the Federal Policy for the Protection of Human Subjects. We hope that these updated outlines continue to be used and updated. Individual researchers and their organizations can do more to ensure safe data transfer if guidelines were easily available and security software less onerous to use.[28] We can act better to secure shared data and once more evidence of safely shared data appears, the better it will be for the medical research enterprise and for patients.

Conclusion

There are many ways to safely share medical data and just as many ways to use data for personal benefit that does not help anyone (e.g., stealing data for personal profit). Although many organizations work on detailed data sharing policies for internal use, it might be time to produce a detailed ethical code specifically for external data sharing, considering the large datasets we use, the mobile applications we create, and the value we might receive from open but appropriately managed data sets.

Fear of data sharing needs to subside when we see the benefits that interoperability of our medical records brings us and we benefit both personally and as a community. The personal genome company 23andme shares data among its participants and some people like that and some people do not. I do not agree with Charles Selfie in *Scientific*

American who wrote in 2013: "It (23andme) is a mechanism meant to be a front end for a massive information-gathering operation against an unwitting public."[29] I think the public is more aware that our data is available in places we might not want it and I would not say we are an unwitting public. We just might need to be better informed by our partners in health care clinics and research and that could happen rapidly if we know more about how our medical data is used.

References

1. Patel V, Hughes P, Savage L, Barker W. Individual perceptions of the privacy and security of medical records. ONC Data Brief No. 27. 2015.
2. Cheung CC, Martin BR, Asa SL. Defining diagnostic tissue in the era of personalized medicine. C Can Med Assoc J. Canadian Medical Association; 2013 Feb 5;185(2):135–9.
3. Ness RB. Influence of the HIPAA Privacy Rule on health research. JAMA. 2007 Nov 14;298(18):2164–70.
4. Collins FS, Varmus H. A new initiative on precision medicine. N Engl J Med. Massachusetts Medical Society; 2015 Jan 30;372(9):793–5.
5. Data Mining - MeSH - NCBI [Internet]. National Center for Biotechnology Information. 2015 [cited 2015 Sep 19]. Available from: http://www.ncbi.nlm.nih.gov/mesh/?term=data+mining
6. Boulton G, Rawlins M, Vallance P, Walport M. Science as a public enterprise: the case for open data. Lancet. 2011;377(9778):1633–5.
7. Drazen JM. Sharing individual patient data from clinical trials. N Engl J Med. Massachusetts Medical Society; 2015 Jan 14;372(3):201–2.
8. Fultz Hollis K. Big data, big sharing, and big security: making medical research data safe to share [BMI 549 unpublished paper]. Oregon Health & Sciences University, Portland, OR; 2014.
9. McGuire AL, Fisher R, Cusenza P, Hudson K, Rothstein MA, McGraw D, et al. Confidentiality, privacy, and security of genetic and genomic test information in electronic health records: points to consider. Genet Med. 2008 Jul;10(7):495–9.
10. Sweeney L, Abu A, Winn J. Identifying participants in the personal genome project by name [Internet]. Available at SSRN 2257732. 2013. Available from: http://dataprivacylab.org/projects/pgp/1021-1.pdf
11. Hunter LE, Hopfer C, Terry SF, Coors ME. Reporting actionable research results: shared secrets can save lives. Sci Transl Med. 2012;4(143):143cm8.
12. Taylor PL, Mandl KD. Leaping the data chasm: structuring donation of clinical data for healthcare innovation and modeling. Harvard Health Policy Rev [Internet]. 2015 Jan [cited 2015 Sep 19];14(2):18–21. Available from: http://www.ncbi.nlm.nih.gov/pmc/articles/PMC4465121/
13. Malin B, Loukides G. Identifiability in biobanks: models, measures, and mitigation strategies. Hum Genet. 2011;130(3):383–92.
14. McCarthy M. University of Minnesota made "serious" ethical errors in trial of antipsychotics, finds report. BMJ. 2015 Jan 24;350(mar24_5):h1628.
15. Fridsma D. EHR interoperability: the structured data capture initiative [Internet]. HealthITBuzz. 2013 [cited 2015 Sep 19]. Available from: http://www.healthit.gov/buzz-blog/electronic-health-and-medical-records/ehr-interoperability-structured-data-capture-initiative/
16. Goozner M. Interoperability—A dream deferred. Modern Healthcare. Crain Communications Inc. (MI); 2015 Apr 20;24.
17. Creswell J. Doctors hit a snag in the rush to connect. [Internet]. New York Times. 2014. p. B1–2. Available from: http://www.nytimes.com/2014/10/01/business/digital-medical-records-become-common-but-sharing-remains-challenging.html
18. Pear R. Tech rivalries impede digital medical record sharing [Internet]. New York Times. 2015 [cited 2015 Sep 19]. Available from: http://www.nytimes.com/2015/05/27/us/electronic-medical-record-sharing-is-hurt-by-business-rivalries.html
19. Health and Human Services Organization. REPORT TO CONGRESS, APRIL 2015 - Report on health information blocking. Washington DC: The Office of the National Coordinator for Health Information Technology (ONC); 2015.
20. HLM. Halamka: 'Probably time to retire the meaningful use construct' [Internet]. HealthLeadersMedia. 2015 [cited 2015 Sep 19]. Available from: http://healthleadersmedia.com/content/TEC-316911/Halamka-Probably-Time-to-Retire-the-Meaningful-Use-Construct.html
21. Ball MJ, Lillis J. E-health: Transforming the physician/patient relationship. Int J Med Inform. 2001;61(1):1–10.

22. Fikes B, Robbins G. Lilly yanks millions from UCSD for Alzheimer's study [Internet]. San Diego Union Tribune. 2015 [cited 2015 Sep 19]. Available from: http://www.sandiegouniontribune.com/news/2015/aug/04/UCSD-Lilly-grants/
23. Basken P. Grant dispute throws an unwritten rule of academic poaching out the window - Research [Internet]. The Chronicle of Higher Education. 2015 [cited 2015 Sep 19]. Available from: http://chronicle.com/article/Grant-Dispute-Throws-an/231857/
24. NIH Guide: Final NIH Statement on Sharing Research Data [Internet]. 2003 [cited 2015 Sep 19]. Available from: http://grants.nih.gov/grants/guide/notice-files/NOT-OD-03-032.html
25. ASHG. American Society of Human Genetics Code of Ethics [Internet]. 2006 [cited 2015 Sep 19]. Available from: http://www.ashg.org/pdf/pol-49.pdf
26. NIH Genomic Data Sharing Policy [Internet]. 2014 [cited 2015 Sep 19]. Available from: http://grants.nih.gov/grants/guide/notice-files/NOT-OD-14-124.html
27. Federal Policy for the Protection of Human Subjects Proposed Changes [Internet]. Federal Register /Vol. 80, No. 173/Tuesday, September 8, 2015/Proposed Rules. 2015 [cited 2015 Sep 19]. Available from: http://www.gpo.gov/fdsys/pkg/FR-2015-09-08/pdf/2015-21756.pdf
28. Ghaith S, Ó Cinnéide M. Improving Software Security Using Search-Based Refactoring. In: Fraser G, Teixeira de Souza J, editors. Search Based Software Engineering SE - 10 [Internet]. Springer Berlin Heidelberg; 2012. p. 121–35. Available from: http://dx.doi.org/10.1007/978-3-642-33119-0_10
29. Selfie C. 23andMe is terrifying, but not for the reasons the FDA thinks [Internet]. Scientific American. 2013 [cited 2015 Sep 19]. Available from: http://www.scientificamerican.com/article/23andme-is-terrifying-but-not-for-reasons-fda/