Published Online October 2010

Biobanks, Privacy, and the Subpoena Power

Teneille Brown[I] and Kelly Lowenberg[II]

I. Genetic Data from Medical Records Can be Subpoenaed by Law enforcement 89
II. HIPAA and the Compelled Disclosure of Medical Records.....90
III. In Practice, Certificates of Confidentiality Provide Ambiguous Protection For Research Data 92
IV. Courts May Balance Constitutional Interests and Compromise Confidentiality 97
V. Conclusion 100

[I] Teneille R. Brown is an Associate Professor of Law at the University of Utah, S.J. Quinney College of Law. At the time of writing this article, she was a fellow with Stanford Law School's Center for Law and the Biosciences and Stanford Medical School's Center for Integration of Research on Genetics and Ethics (CIRGE).
[II] Kelly Lowenberg is a fellow with Stanford Law School's Center for Law and the Biosciences. At the time of writing this article, she was a J.D. candidate at Stanford Law School.

I. GENETIC DATA FROM MEDICAL RECORDS CAN BE SUBPOENAED BY LAW ENFORCEMENT

After 31 years of eluding the Wichita, Kansas police, Dennis Rader was arrested in 2005 and charged with ten counts of murder. Rader, otherwise known as the serial killer BTK (for bind, torture, kill) became a suspect when he began corresponding with the police through discs that contained metadata identifying a computer he had been using at his church. Even though this indirect evidence pointed to Rader, his daughter's medical records ultimately sealed the deal. The police subpoenaed his daughter's pap smear from a local clinic and compared DNA from the sample to semen found at BTK's first crime scene. There was a familial match. The police finally had enough to make an arrest.[1]

This case presents important questions for those of us concerned with the privacy protections surrounding stored genetic samples. As individuals consider contributing their specimen to a bio-repository, or unveiling their medical records for research purposes, they should know what downstream privacy protections exist to protect their personal genetic and medical information. We focus here on genetic samples contained in blood or saliva, but many of the same privacy concerns would attach to other types of biological materials.

There are a few places where genetic samples could reside: in a health care clinic, in a research laboratory, or in an independent biobank.[2] Biobanks can be thus affiliated with a public health department,[3] a health care provider like Kaiser Permanente,[4] or they could be entirely private and not connected to the delivery of health care.[5] By linking large-scale biobanks with individual medical records, researchers hope to uncover critical information regarding the development and expression of complex genetic traits. But, biobanks may also be tapped for another purpose: law enforcement may seek to subpoena genetic samples from biobanks to confirm the identity of suspects of crime or victims of disaster. What must law enforcement demonstrate before they may access this information? A reasonably good suspicion that a serial

---

[1] Ellen Nakashima, *From DNA of Family, a Tool to Make Arrests Privacy Advocates Say the Emerging Practice Turns Relatives Into Genetic Informants*, WASHINGTON POST, April 21, 2008, at A01.

[2] A biobank is a term used to describe a repository that collects, stores and processes biological specimen. In this paper we will focus on human biobanks that collect and store genetic samples.

[3] Newborn screening bloodspots provide a rich resource for valuable population genetics research. The social utility of using this data must be balanced against the privacy concerns, however. In most cases the parents did not assent to their children becoming research subjects or having their data used in any way other than to track the efficacy of the screening program. *See* Aaron Goldenberg, Ethics at the Crossroads of Public Health and Biobanking: The Use of Michigan's Residual Newborn Screening Bloodspots for Research (Jan. 2009) (unpublished Ph.D. dissertation, Case Western Reserve University), *available at* http://en.scientificcommons.org/39294071.

[4] Erika C. Hayden, *Health Organization Lays Plans for Major Biobank*, NATURE 457, 16 (2009), doi:10.1038/457016d.

[5] In many cases, individuals who donate to private biobanks will be asked to waive any property rights that they might have in the samples that they donate. This has created problems with incentives, as subjects may see little community or individual benefit in contributing their sample. David Winickoff has put forward an alternative model for collecting, owning and using genetic specimen to align incentives in a way that makes the biobank and the donor more like partners rather than adversaries. One possibility involves creating a public-private partnership where the biobank acts as fiduciary and holds the donor's samples in a charitable trust. *See* David E. Winickoff & Richard N. Winickoff, *The Charitable Trust as a Model for Genomic Biobanks*, 349 NEW ENG. J. MED 1180, 1180-84 (2003). Hank Greely also proposed a framework for regulation that recognized the need for the biobank to share the benefits with donors. *See generally* Hank Greely, *Breaking the Stalemate: A Prospective Regulatory Framework for Unforeseen Research of Human Tissue Samples*, 34 WAKE FOREST. L. REV. 737 (1999).

killer is in their crosshairs? Or will a simple hunch suffice?[6] This is the primary question we address in this paper. As it turns out, the answer will depend on the purpose for which the genetic specimen was obtained.

II. HIPAA AND THE COMPELLED DISCLOSURE OF MEDICAL RECORDS

When law enforcement would like to order the production of genetic specimen contained in a medical record, the law is fairly clear about what they need to demonstrate. There is no balancing test that law enforcement must apply, no amount of reasonable suspicion or probable cause that they must show. In order to obtain such samples from a patient's ordinary health care records, law enforcement only needs to find that the information sought is relevant to a law enforcement investigation.[7]

The Health Insurance Portability and Accountability Act ("HIPAA") shields patients' protected health information from unauthorized disclosure.[8] Protected health information includes any information that "[i]s created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse" and "[r]elates to the past, present, or future physical or mental health or condition of an individual."[9] The sections dealing with the privacy of medical information have been referred to collectively as "The Privacy Rule."[10] HIPAA only applies to health plans, health care providers, and business associates of health care providers (a "covered entity").[11] A covered entity that discloses the protected health information of her patient without the patient's consent would be subject to HIPAA's sanctions.[12] This is in addition to any professional penalties or tort liability that might be imposed.

HIPAA applies to clinical research conducted by a covered entity, and also to research

---

[6] A few questions that bubble to the surface are: 1) what must the state demonstrate to show that "reasonable efforts" were made to ensure the subject of interest had a chance to object?, and 2) how tangential can the law enforcement use be; *i.e.,* can it be used in asylum hearings or proceedings at Guantanamo Bay? For a review of similar questions, see Mark A. Rothstein & Meghan K. Talbott, *The Expanding Use of DNA in Law Enforcement: What Role for Privacy*?, 34 J.L. MED. & ETHICS 153, 157-58 (2006).

[7] The target of the subpoena is entitled to notice, so that she can challenge the disclosure on relevance or privileged grounds, but some courts will not see the evidentiary privileges as attaching unless the genetic sample would be introduced into the record as evidence. Christopher Slobogin, *Transaction Surveillance by the Government*, 75 MISS. L.J. 139, 158 (2005).

[8] The Health Insurance Portability and Accountability Act, ("HIPAA"), 42 U.S.C. § 1301 et seq., as amended, was enacted by Congress in 1996.

[9] 45 C.F.R. pt. 164.501 (2009).

[10] The Privacy Rule as called for by this Act, includes the proscription of covered entities' disclosure of protected health information, and was implemented as the "Standards for Privacy of Individually Identifiable Health Information," 45 C.F.R. pt. 160-164 (2002).

[11] HIPAA defines a "covered entity" as a health plan, a health care clearinghouse, or a health care provider who transmits any health information in electronic form in connection with a HIPAA transaction. *See* 45 C.F.R. pt. 160.103 (2007).

[12] HIPAA's fines can include civil penalties of up to $100 per occurrence, and criminal penalties starting at $50,000 and up to one year in prison for improperly and knowingly obtaining or disclosing individual health information, to $250,000 and up to ten years in prison for profiting from the improper disclosure of a patient's protected health information. HIPAA § 1177, 42 U.S.C. §§ 1320d-5–1320d-6. *See also* http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/moneypenalties.pdf; and Memorandum from Steven G. Bradbury, Principal Deputy Assistant Attorney General, Office of Legal Counsel to the General Counsel, Department of Health and Human Services, and the Senior Counsel to the Deputy Attorney General, Scope of Criminal Enforcement under 42 U.S.C. § 1320d-6 (June 1, 2005), http://www.usdoj.gov/olc/hipaa_final.htm.

that is not conducted by a covered entity, but that involves the collection of protected health information.[13] Before a researcher could disclose health information that is coupled with health records, specific authorization by the patient is required, unless explicit criteria are met.[14] For example, researchers can use protected health information without the individual's consent if he or she is dead. This is an important carve-out for biobanks, as many of the specimens may belong to individuals who are no longer living. In this case, the covered entity needs to obtain proof from the researcher that the individual is in fact deceased. The researcher must also represent that the disclosure is sought only for research on the health information of the dead person and the information is necessary for the research.[15] Given that genetic material of the deceased may implicate the privacy concerns of his living descendents or the deceased's own personal legacy, this provision of HIPAA may dissuade some from contributing to a biobank that relies only on HIPAA's protections. More broadly, HIPAA does not apply to clinical research if the existing data is de-identified, meaning that the data has been stripped of all identifying information that was originally collected (such as name, birth date, or medical record number), and then it is coded such that the de-identified information cannot be linked back to the individual by the researcher.[16]

Despite this regulatory carve-out for existing, de-identified data, privacy scholars have questioned whether it is ever possible to truly de-identify genetic samples. Researchers have demonstrated the clever ability to both pick individual profiles out of a mixed sample database and to use less than 100 single-nucleotide mutations to uniquely identify an individual or predict his relationship to historical figures.[17] Given the possibility of re-identifying the de-identified

---

[13] *See* NATIONAL INSTITUTES OF HEALTH, DEPARTMENT OF HEALTH AND HUMAN SERVICES, CLINICAL RESEARCH AND THE HIPAA PRIVACY RULE (2004), http://privacyruleandresearch.nih.gov/clin_research.asp.

[14] *Id*. Authorization is not required if a covered entity discloses the information for research if it is being used to: (a) develop the protocol for institutional review board (IRB) approval, (b) for research solely on a decedent's information, (c) if the covered entity receives appropriate documentation that an IRB has granted a waiver or alteration of the authorization requirement, (d) if the protected health information has been de-identified in accordance with the standards set by the Privacy Rule, (e) if the information is released in the form of a limited data set, with certain identifiers removed and with a data use agreement between the researcher and the covered entity, or (f) under a "grandfathered" informed consent of the individual to participate in the research.

[15] 45 C.F.R. § 164.512 (2009).

[16] This only applies to information that is not gathered prospectively through interaction with living individuals. *See* 45 C.F.R. § 46.102(f) (2009) (Institutions are free to use the OHRP guidelines as a floor, rather than a ceiling).

[17] Novel bioinformatics techniques have coupled de-identified individual genetic samples with public geneology records to identify individual pedigrees from haplotype data. *See generally* J. Gitschier, et al., *Inferential Genotyping of Y Chromosomes in Latter-Day Saints Founders and Comparison to Utah Samples in the HapMap Project*, 84 AM. J. HUM. GENETICS, 251, 251-258 (2009). Researchers have also been able to identify individuals from mixed samples. "According to Commander Brent Vermeer, director of the Phoenix Police Department crime lab, much DNA evidence is rendered useless because of contamination and that to eventually put [this] theoretical research into a cost-effective police practice 'would be an amazing asset.'" Press Release, Translational Genomics Research Institute, TGen Scientists Uncover New Field of Research That Could Help Police in Crime Scene Forensics (Aug. 28, 2008), *available at* http://www.tgen.org/news/index.cfm?pageid=57&newsid=1204. *See also* Nils Homer et al., *Resolving Individuals Contributing Trace Amounts of DNA to Highly Complex Mixtures Using High-Density SNP Genotyping Microarrays,* 4 PUB. LIB. SCIENCE GENETICS 1, 2. (2008) ("We demonstrate an approach for rapidly and sensitively determining whether a trace amount . . . of genomic DNA from an individual is present within a complex DNA mixture"); Zhen Lin, Art B. Owen & Russ B. Altman, *Genomic Research and Human Subject Privacy*, 305 SCIENCE 183, 183 (2006) ("One approach to protecting privacy is to limit the amount of high-quality data released and randomly to change a small percentage of SNPs for each subject in the database . . . Our estimates show that measuring as few as 75 statistically independent SNPs would define a small group that contained the real owner of the DNA."); Amy McGuire, *Identifiability of DNA Data: The Need for Consistent*

data, NIH acknowledged that the current privacy protections for genome wide association studies were not enough.[18] Others still argue that there is a need for more protection, in the form of federal regulation.[19]

While HIPPA created a statutory framework that prohibits health care workers from voluntarily disclosing a patient's health care information, HIPAA provides no barrier to the involuntary disclosure of a patient's information pursuant to a subpoena. In fact, the rules promulgated under HIPAA expressly allow it.[20] Unauthorized disclosure of an individual's protected health information can occur in response to a subpoena, a simple discovery request, or any other lawful process, even without a court order. The health plan or provider just needs to be assured that the party seeking the information has made reasonable efforts to notify the patient of the request.[21] This is the situation presented by the BTK killer story above, as Rader's daughter only needed to be notified that the police were subpoenaing her pap smear specimen.

III. IN PRACTICE, CERTIFICATES OF CONFIDENTIALITY PROVIDE AMBIGUOUS PROTECTION FOR RESEARCH DATA

Now, we leave the realm of pure health care delivery and turn to the realm of research. As the Institute of Medicine has recently pointed out in its report, *Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research*, the HIPAA Privacy Rule "does not protect privacy as well as it should, and . . ., as currently implemented, it impedes important health research."[22] HIPAA does not apply neatly in the research setting, as the privacy regulations were originally designed to protect health information that is processed electronically by providers and insurance companies.

Investigators need to be especially cautious about protecting research subjects' privacy rights particularly because subjects already have so many incentives not to enroll in a clinical trial. Among the factors that may limit subject participation in research are low financial rewards and considerable inconveniences of participating with potentially no other benefit. The payment or token incentive to the subject is capped so it is not deemed too coercive. Additionally, the subject may be receiving a placebo. She may be given something that is not effective, and the study protocol may be onerous. If we add to this list that her genetic information may be disclosed and could incriminate her in a court of law, our ability to effectively recruit subjects for research becomes even more difficult. In part because of these

---

Federal Policy, 8 AM. J. BIOETHICS 75 (2008).

[18] Matt Jones, *Forensic Breakthrough Stirs NIH to Close GWAS Data from Public View*, GenomeWeb Daily News, Aug. 29, 2008, http://www.genomeweb.com/forensic-breakthrough-stirs-nih-close-gwas-data-public-view ("NIH … removed aggregate statistics files of individual GWAS studies, including the Database of Genotypes and Phenotypes (dbGaP), run by the National Center for Biotechnology Information, and the Cancer Genetic Markers of Susceptibility database, run by the National Cancer Institute . . . That data is still available for use by researchers who apply for access to the data and agree to protect its confidentiality using the same approach they do for individual-level study data").

[19] McGuire, *supra* note 17.

[20] 45 C.F.R. § 164.512 (2009); In *U.S. ex rel. Steward v. Louisiana Clinic*, the court held that information acquired through broad discovery authorization may be used for purposes beyond the context of health care fraud litigation. 2002 WL 31819130 (E.D. La. 2002).

[21] 45 C.F.R. § 164.512 (2009).

[22] INSTITUTE OF MEDICINE OF THE NATIONAL ACADEMIES OF SCIENCES, REPORT BRIEF: BEYOND THE HIPAA PRIVACY RULE: ENHANCING PRIVACY, IMPROVING HEALTH THROUGH RESEARCH 1 (2009) *available at* http://www.iom.edu/?id=61836 (follow the "Start download" link).

concerns, we have a separate system for protecting subjects' sensitive information: the Certificate of Confidentiality.

Certificates of Confidentiality are issued by the National Institutes of Health (NIH) to protect identifiable research information from forced disclosure to anyone,[23] including law enforcement. The protection only applies to research, and cannot be used to protect from forced disclosure of purely clinical information. The history of the certificates dates back to 1970, when the Comprehensive Drug Abuse Prevention and Control Act (Drug Abuse Act)[24] amended the Public Health Service Act ("the Act") to grant the Secretary of the Department of Health Education and Welfare (now the Department of Health and Human Services) the authority to protect from subpoena any identifying information about subjects enrolled in studies of drug use and abuse.[25] In 1974, that protection was extended to research on mental health,[26] and in 1988, the provision[27] was changed to its current form, whereby the Secretary of the Department of Health and Human Services (HHS) authorized researchers to refuse to disclose any sensitive identifying information on research participants in civil, criminal, administrative, legislative, or other legal proceedings, whether state, federal, or local.[28] The Secretary of HHS subsequently delegated power to implement this provision to the NIH and other HHS agencies.

There are several limitations to the privacy protections that a Certificate grants, some of which are better established than others. In contrast to the thoroughly examined HIPPA protections Certificates of Confidentiality have remained relatively untested in the courts. As a result, individual subjects may perceive them as guaranteeing more robust privacy protection than they may actually provide.

Starting with the most established limitation on the Certificate, information is protected from subpoena only if the project for which that information is collected and maintained has been granted a Certificate of Confidentiality. An institution can be granted a Certificate of Confidentiality for a project if the project is research-based or research-related, has been reviewed by an Institutional Review Board (IRB),[29] collects personally identifiable information,

---

[23] Disclosures are made for a few exceptions: CDC and FDA reporting, audits, and the participant's request.
[24] Pub. L. No. 91-513, §3(a).
[25] *Id.*
[26] Comprehensive Alcohol Abuse and Alcoholism Prevention, Treatment, and Rehabilitation Amendments of 1974, Pub. L. No. 93-282, §122(b).
[27] Health Omnibus Programs Extension of 1988, Pub. L. No. 100-607, §163 (codified as amended at 42 U.S.C. § 241(d), 301(d)).
[28] *Id.* (Authorizing persons engaged in biomedical, behavioral, clinical, or other research (including research on mental health, and research on the use and effect of alcohol and other psychoactive drugs) to protect the privacy of individuals who are the subject of such research by withholding from all persons not connected with the conduct of such research the names or other identifying characteristics of such individuals. Persons so authorized to protect the privacy of such individuals may not be compelled in any Federal, State, or local civil, criminal, administrative, legislative, or other proceedings to identify such individuals).
[29] In response to the human subjects research disasters of the 1960s and 1970s, the federal government made it mandatory to have an independent, institutional review board approve study design and protocols, to make sure that the safety of human subjects was protected. Two separate threads developed, one imposing regulations on all HHS-funded research, *see* 45 C.F.R. § 46.101, and a separate IRB process for Food and Drug Administration-related clinical trial research, *see* 21 C.F.R. pt. 56. An IRB is "an appropriately constituted group that has been formally designated to review and monitor biomedical research involving human subjects." FOOD AND DRUG ADMINISTRATION, GUIDANCE FOR INSTITUTIONAL REVIEW BOARDS AND CLINICAL INVESTIGATORS 1998 UPDATE (1998), http://www.fda.gov/oc/ohrt/irbs/faqs.html.

and that information could cause significant harm or damage to the participant if disclosed.[30] According to federal regulations, research means "a systematic investigation, including research development, testing and evaluation, designed to develop or contribute to generalizable knowledge."[31] The implementing regulations listed illustrative examples of the types of sensitive information that can be protected, and among this list was drug use, HIV status, or genetic information. It is important to note that Certificates therefore do not apply to many categories of research that do not collect "sensitive" information. Unlike other federal protections of human subjects research, receiving federal funding is not required for a study to be eligible for a Certificate. While the NIH posts detailed instructions as to what is required to obtain a Certificate,[32] approval by the NIH is discretionary and there is no reported data on why a project may be denied a certificate.[33]

The Certificate protects the names and identifying characteristics of research subjects. According to HHS, an identifier is any information that can link specimens or data to living people or their medical information. Guidance documents put out by HHS make plain that genetic information is also caught under the heading of "identifying characteristics."[34] Investigators conducting genomic research also often collect non-genetic information about the subject (age, gender, types of medications consumed, location, medical diagnoses, behavioral characteristics). This non-genetic data is also protected if it, alone or in combination with other data, "could reasonably lead, directly or indirectly by reference to other information, to identification of that research subject."[35]

If a project to build a biobank is granted a Certificate of Confidentiality, all of the accompanying information that could be used to identify a participant is therefore protected. Permanent protection attaches to any information collected during the effective window after the Certificate becomes effective and before it expires. Multi-site projects can also be granted a Certificate, so long as the application to NIH contains a brief description of the facilities and personnel who will be involved in the conduct of the research. The lead site should apply for a single Certificate to protect the research participants enrolled at all of the sites. If new sites are

---

[30] Specifically, information may be deemed sensitive and protected if it could be damaging to the subject's financial standing, employability, insurability, or reputation if an accidental breach of confidentiality were to occur. NATIONAL INSTITUTE OF GENERAL MEDICAL SCIENCES, CERTIFICATES OF CONFIDENTIALITY: NIGMS PROCEDURES (2003), http://www.nigms.nih.gov/Research/Bioethics/CertConf.htm.

[31] 45 C.F.R § 46.102(d).

[32] Among other things, the application must include a description of the means used to protect subjects and identities, the reasons for requesting a Certificate of Confidentiality, approval by an IRB, and the informed consent protections contained in the IRB approval process. "The informed consent form must include a description of the protections and limitations of the Certificate of Confidentiality, including the circumstances in which the investigators plan to disclose voluntarily identifying information about research participants (e.g., child abuse, harm to self or others, etc.)" See the *Detailed Application Instructions for Certificates of Confidentiality: Extramural Research Projects,* on the National Institutes of Health website, http://grants2.nih.gov/grants/policy/coc/appl_extramural.htm.

[33] Visit the U.S. Department of Health and Human Services' web kiosk, discussing the details of Certificates of Confidentiality, at http://grants.nih.gov/grants/policy/coc/.

[34] Identifying characteristics include things such as: name, address, social security or other identifying number, fingerprints, voiceprints, photographs, genetic information or tissue samples, or any other item or combination of data about a research participant which could reasonably lead, directly or indirectly by reference to other information, to identification of that research subject. NATIONAL INSTITUTES OF HEALTH, DEPARTMENT OF HEALTH AND HUMAN SERVICES, FREQUENTLY ASKED QUESTIONS ON CERTIFICATES OF CONFIDENTIALITY (2002), http://grants.nih.gov/grants/policy/coc/faqs.htm.

[35] *Id.*

added after the Certificate is issued, the lead site should provide NIH with an updated list of affiliated personnel.[36] If researchers disclose unauthorized genetic information to personnel who are not listed in the initial application or its amendments, then the confidentiality has been breached and the Certificate will not protect the unauthorized person from compelled disclosure.

The NIH guidance documents warn that Certificates of Confidentiality do not take the place of good practices related to data security. Researchers are counseled to "take appropriate steps to safeguard research data and findings. Unauthorized individuals must not access the research data or learn the identity of research participants."[37] Researchers can avoid this potential problem and comply with the NIH guidance by only sharing de-identified data through the biobank. With genetic information, the question is whether data can ever be completely de-identified, as we saw above where researchers identified unique individuals from a genome wide association study that contained a mixture of many samples.

Although it is easy enough to remove a subject's name from the sample and code the data, other characteristics about the person from whom the sample was taken would make the genetic information more useful to other researchers. Such information often includes age, gender, medications taken, diagnosed diseases, date of sample donation, and zip code. These pieces of non-genetic information can be cross-referenced with publicly available databases, like voter registration records and the telephone book, and used to re-identify the genetic information. This risk increases, if the biobank is smaller or more specific, drawing from a targeted population or studying a rare disease.

Specimen from the biobank could provide genetic information from which one could infer an individuals' "gender, blood type, approximate skin pigmentation, and manifestations of Mendelian disorders."[38] The richness of this identifying information will increase as our ability to determine complex phenotypes from cheap genetic testing chips improves.[39] Depending on the size of the biobank, among other things, this information could be used to identify a participant. Given the cases of re-identification that were discussed above, even if genetic samples are completely scrubbed of other information, they may never be truly de-identified.

Investigators who are authorized to resist compelled disclosure can only protect a participant's privacy as it pertains to the research project. Investigators who combine their research with individual patient care run the risk of waiving the Certificate's protections if the research data becomes commingled with an individual's health records. The Certificate does not protect patients; it protects study participants.[40] Although, in reality, it is quite common for a person to simultaneously be both a research participant and a medical patient, researchers should keep records as if the patient/subject were two different people, separating the protected research information from the unprotected medical records.

Even if data receives the full protections of a Certificate of Confidentiality, the researcher or her institution can voluntarily disclose the data. Voluntary disclosure may occur for a number

---

[36] NATIONAL INSTITUTES OF HEALTH, DEPARTMENT OF HEALTH AND HUMAN SERVICES, DETAILED APPLICATION INSTRUCTIONS FOR CERTIFICATE OF CONFIDENTIALITY: INTRAMURAL RESEARCH PROJECTS (2002), http://grants.nih.gov/grants/policy/coc/appl_intramural.htm.

[37] NATIONAL INSTITUTES OF HEALTH, DEPARTMENT OF HEALTH AND HUMAN SERVICES, CERTIFICATES OF CONFIDENTIALITY: BACKGROUND INFORMATION (2003), http://grants.nih.gov/grants/policy/coc/background.htm.

[38] William W. Lowrance & Francis S. Collins, *Identifiability in Genomic Research*, 317 SCIENCE 600, 601 (2007).

[39] Fan Liu, et al., *Eye Color and the Prediction of Complex Phenotypes from Genotypes*, 19 CURRENT BIOL., R192, R192-R193 (2009).

[40] C. L. Earley & Louise Strong, *Certificates of Confidentiality: A Valuable Tool for Protecting Genetic Data*, 57 AM. J. HUMAN GENETICS 727, 730 (1995).

of reasons, for example, one may feel a moral compulsion to aid a criminal investigation, or prefer avoiding the financial or personal toll of contesting the subpoena. Although an investigator may wish to contest the subpoena, perhaps because she feels a duty to protect the participants whose data she has collected, the Certificate is granted to the institution,[41] not to the investigator. The ultimate decision thus lies with the institution sponsoring the research, which may be more concerned by the prospect of an expensive legal battle.

Federally funded institutions, however, are required by their IRBs to give participants informed consent including an explanation thorough enough to allow a participant to decide whether or not she wants to assume the risks of the research. The level of confidentiality and privacy promised to that participant is one part of the informed consent. Two questions that remain are (1) what information did the subject consent to be disclosed, and (2) should a subject be allowed to waive consent for future, unanticipated uses of their data.[42] If a researcher states that she would disclose any information under subpoena, then she will be able to. If she states the research data will not be revealed to anyone, then she is contractually obligated not to voluntarily disclose the information, at the risk of private lawsuits or regulatory violations.

As noted above, private biobanks that do not receive government funding are still eligible for a Certificate if an IRB has given assurances that the protocol sufficiently protects human subjects. This is true even though the federal policies such as the Common Rule[43] and HIPAA do not apply to institutions that do not receive any federal funds. One would hope that a private company seeking IRB approval would receive the same level of scrutiny over its informed consent process as a federally funded laboratory. We would also hope that private biobanks that do not receive federal funds would voluntarily comply with the Common Rule and HIPAA, despite there not being any legal requirement to do so. Some of the larger players in this market will likely voluntarily comply with these federal standards so that they engender goodwill and broader marketability. However, there will no doubt be fly-by-night biobanks that are not as vigilant in protecting human subjects.

Even so, there is some concern that privately funded biobanks can shop around for a for-profit IRB that will simply rubberstamp its projects.[44] While conflicts of interest exist in not-for-profit IRBs as well, the concerns are compounded in a for-profit model, as the financial incentives for securing a long-term partnership between the parties grows. In any event, ideally, any IRB should require that consent forms clearly state the institution's intent to comply or resist subpoenas for the participant's information. But, regardless of the informed consent requirement, the reality of the informed consent process may lead the subject to accidentally waive her privacy rights. Consent forms for collecting biospecimens are often tens of pages long, and participants may not read or remember all of the information, including the project's

---

[41] Laura M. Beskow, Lauren Dame, & E. Jane Costello, *Certificates of Confidentiality and Compelled Disclosure of Data*, 322 SCIENCE 1054, 1055 (2008).

[42] Ellen Wright Clayton, *Informed Consent and Biobanks*, Symposium Issue of the J.L. MED. & ETHICS 15, 20 (2005).

[43] The Common Rule is a federal policy that has been enacted by HHS and FDA and requires that the risk to human subjects be mitigated, and their privacy protected, through informed consent. *Basic HHS Policy for Protection of Human Research Subjects*, 45 C.F.R pt. 46 (2009).

[44] "[F]or-profit research ethics boards are in a client–provider relationship with study sponsors; this relationship creates a conflict of interest; and this conflict of interest is particularly dangerous under a weak regulatory system which does not prevent forum shopping and allows market criteria to influence committee selection." Trudo Lemmens & Carl Eliott, *Research Ethics Boards: Reply from Trudo Lemmens and Carl Elliott*, 3 PUB. LIB. SCIENCE MED. 1968, 1970 (2006).

privacy policy.

IV. COURTS MAY BALANCE CONSTITUTIONAL INTERESTS AND COMPROMISE CONFIDENTIALITY

Having established the limits of the statutory framework, we turn to how the Certificate fares in court when a researcher resists a subpoena. There are very few appellate cases in which a subpoena of information protected by a Certificate has been challenged. The first such case, *New York v. Newman*,[45] involved the identity of people participating in a drug treatment program. Although *Newman* is not about research, it relies on the same 1970 amendment[46] to the Public Health Service Act ("the Act")[47] that originally authorized the Certificate of Confidentiality.[48] *Newman* establishes that the confidentiality protections housed in the Act can guard against a subpoena.

Newman deals with a situation in 1972, in which a witness to a shooting claimed she had previously seen the shooter in the waiting room of the New York City Methodone Maintenance Treatment Program. The police subpoenaed photographs of patients from the treatment program, and the director, Dr. Robert Newman, refused to produce the photos.[49] The New York State Court of Appeals decided that Dr. Newman did not have to produce the photographs, citing to the 1970 amendment to the Act.[50] *People v. Newman* demonstrates that the protection against involuntary disclosure in Section 301(d) of the Act can defend against a subpoena, when that subpoena is issued by the prosecution and requests information that will easily identify participants, such as photographs.

More recently, a 2004 case in North Carolina demonstrates the questionable legal status of modern Certificates of Confidentiality, particularly when a criminal defendant asserts a due process right to subpoena the otherwise confidential records.

In *North Carolina v. Bradley*,[51] the defendant attempted to subpoena research records from a Duke University Health System (Duke) study on psychiatric disorders that was protected by a Certificate of Confidentiality. In the case, the criminal defendant was accused of two counts of indecency with a minor and one count of statutory rape. The defendant believed that a witness for the prosecution, who testified at trial that she had also been molested by the defendant, had participated in this Duke study. Before trial, defense counsel issued a subpoena to Duke seeking

---

[45] *New York v. Newman*, 32 N.Y. 2d 379, 382 (1973).

[46] Comprehensive Drug Abuse Prevention and Control Act Pub. L. No. 91-513, §3(a), (1970), 42 U.S.C § 242(a).

[47] 42 U.S.C § 241(d).

[48] *Newman* deals with medical information, but Certificates of Confidentiality do *not* protect medical information. The protection for the Methodone treatment facility in *Newman* is governed by a different regulation. Conditions for the Use of Methadone, 37 Fed. Reg. 26800 §130.44 (b)(13)(ii)(e)(3)(g)(2) (December 15, 1972) (codified at 21 C.F.R. § 130.44).

[49] The subpoena was "specifically drawn to obtain relevant material that is not privileged by State law . . . The identification-card photographs of methadone patients in the New York City Methadone Maintenance Treatment Program are not confidential privileged information protected by [State law.]" *New York v. Newman*, 32 N.Y. 2d 379, 381 (1973).

[50] As you recall, the Certificate of Confidentiality provisions under the Drug Abuse and Office and Treatment Act of 1972 were later expanded to include other types of sensitive health information. But even before that, the 1970 Act was revised by the 1972 Act. The 1970 Act gave absolute protection to drug research programs, and that was not revised by the 1972 Act, which applied to "drug abuse prevention functions." *New York v. Newman*, 32 N.Y. 2d 379, 384-385, 389-90 (1973).

[51] *See generally North Carolina v. Bradley*, 634 S.E.2d 258 (2006).

"any and all documents from the [psychiatric study] recording, reflecting or referencing any statement by [the witness] . . . mentioning or describing any abuse of her."[52] The defendant was apparently on a fishing expedition for any prior inconsistent statements about her abuse. Duke argued that the Certificate protected the confidentiality of the study data and its disclosure could not be compelled. The trial court granted Duke's motion for a protective order, and required Duke to maintain a sealed copy of the records in case defendant appealed.[53]

The defendant was convicted, and he appealed. In order "to ensure a full and fair appellate review," defendant argued that he needed to have access to the research documents that had been sealed by the trial court's protective order. The trial court agreed, and ordered Duke to produce the records for defendant's appellate counsel. The contents were not to be disseminated to anyone other than parties' attorneys. Duke appealed from this order, and without acknowledging that the witness had participated in the study, Duke asserted that the information was not about the defendant, and therefore was unlikely to include exculpatory evidence.

The defendant argued that the trial court "was required, at the very least, to review the records *in camera* to determine if there was exculpatory evidence contained therein."[54] However, as the Court of Appeals for North Carolina properly pointed out, "just because defendant asks for an *in camera* inspection does not automatically entitle him to one. Defendant still must demonstrate that the evidence sought to be disclosed might be material and favorable to his defense."[55] In this case, the witness was only one of three witnesses who provided testimony, which was subject to cross-examination. Considered in the context of the other evidence, the Duke research records were not considered material to the outcome of the case. The appeals court found that Duke was correct to fight the order to disclose the research records,[56] and that the trial judge did not have to review the records *in camera* because the defendant had not shown how the records might be material. The court therefore did not need to reach the issue of whether due process rights would compel the confidential records to be reviewed *in camera*. The appeals court then vacated the trial court's order.[57]

This case ultimately came to the correct conclusion, but only after Duke fought a lengthy battle through the appeals process. If Duke had not continued to fight the trial court's order, then the records would have been viewed by the defense counsel, and perhaps others. However, if the defendant in the case had made a showing that the evidence might be material to the outcome of his case, the court would have had to engage in a balancing act between statutory and constitutional rights. Defendants have a limited constitutional right to subpoena exculpatory evidence. This right is derived both in the Sixth Amendment's provision for criminal defendants

---

[52] *Id.* at 260.
[53] *Id.*
[54] *Id.* at 263.
[55] *Id.* at 262. Note that evidence is material only "'if there is a reasonable probability that, had the evidence been disclosed to the defense, the result of the proceeding would have been different. A 'reasonable probability' is a probability sufficient to undermine confidence in the outcome.'" *Id*., citing *United States v. Bagley,* 473 U.S. 667, 682 (1985) in *North Carolina v. Tirado*, 599 S.E.2d 515, 541 (2004).
[56] The appeals court established that a researcher has the right to appeal a subpoena as "a 'party aggrieved' [because] [t]he trial court's order effectively requires DUHS to disclose information concerning the research subject's privacy which it is obliged, pursuant to the Certificate of Confidentiality and federal statutes, to protect." *North Carolina v. Bradley*, 634 S.E.2d at 262.
[57] "[E]xtrinsic evidence of prior inconsistent statements may not be used to impeach a witness where the questions concern matters collateral to the issues. Such collateral matters have been held to include testimony contradicting a witness's denial that he made a prior statement when that testimony purports to reiterate the substance of the statement." *Id*. at 262-3.

to have "compulsory process for obtaining witnesses in his favor"[58] and the Fourteenth Amendment's provision that no state "deprive any person of life, liberty, or property, without due process of law."[59] The Supreme Court case of *Pennsylvania v. Ritchie*[60] provides some guidance on how this statutory privilege and constitutional balancing act might play out in courts. We will turn to that case now.

George Ritchie was convicted of raping his 13-year old daughter, who testified at his trial and was cross-examined. On appeal, Ritchie argued he should have been able to subpoena the records of his daughter's conversations with Children and Youth Services ("CYS"), a state protective agency that investigates cases of child abuse and neglect. The defendant wanted to search these records for any inconsistent statements that may have been made by his daughter, and to better target his cross-examination of her testimony. He claimed the trial court's denial of his subpoena violated the Sixth Amendment compulsory process and confrontation clause rights, and also violated his Fourteenth Amendment due process right.

The plurality opinion held that the confrontation clause did not apply to this question of compelled disclosure of confidential information to the defendant, as it only protects a defendant's trial rights, and "does not compel the pretrial production of information that might be useful in preparing for trial."[61] The *Ritchie* plurality held that the judge could not have prevented Ritchie's lawyer from cross-examining his daughter, but otherwise the confrontation clause did not apply.

This Court also decided not to rely on the compulsory process clause of the Sixth Amendment, as it provides no greater protection than the Fourteenth Amendment, and the due process clause is better developed and sufficient on its own. Even so, the plurality opinion mentioned that the Court has never squarely held that compulsory process guarantees the absolute right to criminal defendants to require the government to produce exculpatory evidence.[62]

Unlike the Act and Certificates of Confidentiality, the statute granting CYS confidentiality had express exceptions including permitting disclosure pursuant to a court order. The Court therefore affirmed the decision of the Pennsylvania Supreme Court, which ordered a remand to determine whether the CYS records were material under the analysis discussed above in *Bradley*.[63] The result is that the defendant is entitled to have the CYS file reviewed by the trial court to determine whether it contains information that would likely have changed the outcome of his trial. However, defense counsel was not permitted to review the confidential contents of the file.[64] The Court "express[ed] no opinion on whether the result . . . would have been different if the statute had protected the CYS files from disclosure to *anyone,* including law-enforcement and judicial personnel" as is the case with Certificates of Confidentiality.[65] Put

---

[58] U.S. Const. amend. VI.
[59] U.S. Const. amend. XIV.
[60] *Pennsylvania v. Ritchie*, 480 U.S. 39 (1987).
[61] *Id*. at 53 n.9.
[62] *Id.* at 56
[63] *Id.* at 58.
[64] *Id.*
[65] *Id*. at 57 n.14. A similar analysis may ensue under state statutes creating disease registries. Although a New York statute provides for "unqualified confidentiality" in connection with participating in a diabetes registry, the protection this accords has also been called into doubt. This suggests that state statutes may not seal off gaps in the privacy protections that Certificates of Confidentiality provide. Harold Krent, et al., *Whose Business is Your Pancreas? Potential Privacy Problems in New York City's Mandatory Diabetes Registry*, 17 ANNALS HEALTH L. 1, 17 (2008).

differently, the Court did not decide whether the constitutional due process protections apply when a statute such as the Act gives absolute confidentiality protections.

Ultimately, the special constitutional protections afforded to criminal defendants may allow them to pierce the Certificates' absolute bar on compelled disclosure, as statutory protections are not as powerful as constitutional ones. Further, in order to answer the question of whether the Certificate could be trumped by due process concerns, upon a showing of materiality, the trial court and defense counsel will typically be allowed to review the records and violate their confidentiality, albeit in a limited manner that is confined to those particular proceedings.

Although the holding in Ritchie, that provided only for *in camera* review of the confidential information by the judge, may deny "[defendant] the benefits of an 'advocate's eye,' . . . [i]f a defendant is aware of specific information contained in the file . . . he is free to request it directly from the court, and argue in favor of its materiality."[66] The rationale for this holding is the same as the rationale for the Act authorizing the Certificate. If the records were made available to defendants, even through counsel, it could have a seriously adverse effect on the institution's ability to get sensitive information from people in order to serve its purpose (*i.e.,* preventing child abuse or researching treatments for genetic disorders).[67]

V. CONCLUSION

Gaps in the Certificate of Confidentiality protections widen when sensitive data, that cannot be fully de-identified, is shared across institutions and used in new projects. Certificates of Confidentiality will also not provide protection when research studies are combined with patient care, and the files are commingled. With some planning, however, these gaps can hopefully be closed. Biobanks concerned with maintaining their protections through a Certificate of Confidentiality should contractually require all people who access the biobank to abide by the same privacy protections promised to the participant during informed consent, whatever those may be. Another path to close this gap is to require all researchers who access the biobank to also obtain Certificates of Confidentiality for their research projects. Biobanks should also keep in mind these potential gaps when deciding what information to share with future research associates. Additionally, with the development of electronic medical records, clinical information should be kept separately from the shielded research information.

Certificates have rarely been tested by the judiciary. No appellate court has decided whether a researcher can rely on a Certificate of Confidentiality to resist subpoena for information that might be material to a criminal defense. Scant case law implies that Sixth Amendment claims may not compel pretrial discovery, but the compulsory process clause and the confrontation clause may be triggered if the prosecution seeks to use genetic information at trial. It is not settled whether due process rights to search for exculpatory evidence can compel pretrial discovery of absolutely privileged records. At this point, not much can be said about how the lower courts will balance the privacy protections accorded in the Act, with the constitutional protections of the Sixth and Fourteenth Amendment.

Even so, what can be said is that the absolute protection that is seemingly accorded by the Certificates of Confidentiality has not yet been echoed in criminal courts. As a result, the Certificates may fall short of their statutory promise, thereby resulting in partial or full disclosure

[66] *Id*. at 60.
[67] *Id*.

of a subject's sensitive research data. Given this reality, protective orders and *in camera* review by judges should be the rule rather than the exception in determining whether the evidence is admissible, relevant, or material. Making it clear that law enforcement and opposing counsel are not guaranteed access to the information protected by the Certificate of Confidentiality will go a long way in preventing fishing expeditions that could stifle future subject recruitment.

This lack of absolute protection under Certificates of Confidentiality is problematic in many research domains. However, it may present a particular stumbling block for biobanking research, as the traditional models for informed consent and subject participation do not apply.[68] Rather than having each individual consent to a particular use of her genetic data, with biobanks you often have individuals consenting (or not, if the information was gathered for a different purpose and the data is de-identified) to research that involves using their genetic material in future, undefined ways, and by researchers they have never met. This is because the subject may only interact with the biobank, which might operate as a go-between supplier of the genetic material to the researchers. Because of the lattice patchwork of entities involved in biobank research, the distribution chain must be airtight in its privacy protections. Given that subjects have no *a priori* reason to trust the downstream researchers who might use their genetic samples, it is of paramount importance that privacy protections for biobanking subjects remain as robust as possible. Concerns over law enforcement abuses will heighten if the entity encouraging the nation-wide collection and sharing of this genetic information is the federal government.[69] Without iron-clad protection against law enforcement subpoena of the genetic data, society will not be able to receive the full public health benefit of large-scale biobanks.

[68] Mark Rothstein, *Expanding the Ethical Analysis of Biobanks*, J.L. MED. & ETHICS 89, 89-94 (2005).

[69] The Genomics and Personalized Medicine Act of 2006 was again introduced to the House of Representatives in July 2008, but it died before becoming law. It did, however, signal a remarkable shift in the discussion surrounding public health and biobanks by calling for a feasibility study for a national biobanking research initiative. For a discussion of this bill, see Helen Swede, Carole Stone, & Alyssa Norwood, *National Population-Based Biobanks for Genetic Research*, 9 GENETICS. IN MED. 141 (2007).