BDK20 – Regulatory Issues in Big Data for Genomics and Health

References

Acquisti, A (2004). Privacy in electronic commerce and the economics of immediate gratification. *Proceedings of the 5th ACM Conference on Electronic Commerce*, New York, NY. Association for Computing Machinery. 21-29.

Acquisti, A and Gross, R (2009). Predicting Social Security numbers from public data. *Proceedings of the National Academy of Sciences*. 106: 10975-10980.

Agaku, IT, Adisa, AO, et al. (2014). Concern about security and privacy, and perceived control over collection and use of health information are related to withholding of health information from healthcare providers. *Journal of the American Medical Informatics Association*. 21: 374-378.

Agrawal, S and Budetti, P (2011). Physician medical identity theft. *Journal of the American Medical Association*. 307: 459-460.

Allan, A (2005). Password Aging Can Burden an Already-Weak Authentication Method. Stamford, CT, Gartner

Anonymous (1997). For the Record: Protecting Electronic Health Information. Washington, DC, National Academies Press.

Anonymous (2002). Secure Hash Signature Standard. Gaithersburg, MD, National Institute for Standards and Technology. http://csrc.nist.gov/publications/fips/fips180-2/fips180-2withchangenotice.pdf

Anonymous (2005). National Consumer Health Privacy Survey 2005. Oakland, CA, California Health Care Foundation. http://www.chcf.org/topics/view.cfm?itemID=115694

Anonymous (2007). Security 101 for Covered Entities. Baltimore, MD, Centers for Medicare and Medicaid Services. http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/security101.pdf

Anonymous (2008). A Delicate Balance: Behavioral Health, Patient Privacy, and the Need to Know. Oakland, CA, California Health Care Foundation. http://www.chcf.org/documents/chronicdisease/ADelicateBalanceBehavioralHealthAndPrivacyIB.pdf

Anonymous (2008). Mitigating medical identity theft. *Journal of AHIMA*. 79(7): 63-69. http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_039058.hcsp?dDocName=bok1_039058

Anonymous (2009). Health Information Bill of Rights. Chicago, IL, American Health Information Management Association. http://www.ahima.org/pr/HI_Bill_of_Rights.pdf

Anonymous (2009). Medical Records Privacy San Diego, CA, Privacy Rights Clearinghouse. http://www.privacyrights.org/fs/fs8-med.htm

Anonymous (2011). Health Information Technology & Privacy. Philadelphia, PA, American College of Physicians. http://www.acponline.org/advocacy/where_we_stand/policy/hit_privacy.pdf

Anonymous (2012). 2012 HIMSS Analytics Report: Security of Patient Data. Chicago, IL, HIMSS Analytics. http://www.krollcybersecurity.com/media/Kroll-HIMSS_2012_-_Security_of_Patient_Data_040912.pdf

Anonymous (2013). The Economic and Productivity Impact of IT Security on Healthcare. Traverse City, MI, Ponemon Institute. http://www.imprivata.com/resources/analyst-reports/ponemon-institute-study-economic-and-productivity-impact-it-security

Anonymous (2013). A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes. Washington, DC, US Senate Committee on Commerce, Science, and Transportation. http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=0d2b3642-6221-4888-a631-08f2f255b577

Anonymous (2013). Summary Report of Qualitative Research into Public Attitudes to Personal Data and Linking Personal Data. London, England, Wellcome Trust. http://www.wellcome.ac.uk/stellent/groups/corporatesite/@msh_grants/documents/web_document/wtp053205.pdf

Anonymous (2013). Update: Privacy and security of protected health information - Omnibus Final Rule and stakeholder considerations. Washington, DC, Deloitte. http://www.deloitte.com/assets/Dcom-UnitedStates/Local Assets/Documents/Center for health solutions/us_lshc_SecurityPrivacyPHI_080913.pdf

Anonymous (2014). 2014 Cost of Data Breach Study. Traverse City, MI, Ponemon Institute LLC. http://www-935.ibm.com/services/us/en/it-services/security-services/cost-of-data-breach/

Anonymous (2014). Annual Report to Congress on Breaches of Unsecured Protected Health Information For Calendar Years 2011 and 2012. Washington, DC, Department of Health and Human Services. http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachreport2011-2012.pdf

Anonymous (2014). The Essential OAuth Primer - Understanding OAuth for Securing Cloud APIs. Denver, CO, Ping Identity Corporation. https://www.pingidentity.com/en/resources/white-papers/oauth-primer.html

Anonymous (2015). 2014 Fifth Annual Study on Medical Identity Theft. Traverse City, MI, Ponemon Institute LLC. http://medidfraud.org/2014-fifth-annual-study-on-medical-identity-theft/

Anonymous (2015). Guide to Privacy and Security of Health Information. Washington, DC, Department of Health and Human Services. http://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf

Appari, A and Johnson, ME (2010). Information security and privacy in healthcare: current state of research. *International Journal of Internet and Enterprise Management*. 6: 279-314.

Barth-Jones, DC (2012). The 'Re-Identification' of Governor William Weld's Medical Information: A Critical Re-Examination of Health Data Identification Risks and Privacy Protections, Then and Now, Social Science Research Network. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2076397

Blumenthal, D and McGraw, D (2015). Keeping personal health information safe - the importance of good data hygiene. *Journal of the American Medical Association*. 313: 1424.

Blythe, J, Koppel, R, et al. (2013). Circumvention of Security: Good Users Do Bad Things. Systems Security

Bobicev, V, Sokolova, M, et al. (2013). Can anonymous posters on medical forums be reidentified? *Journal of Medical Internet Research*. 15(10): e215. http://www.jmir.org/2013/10/e215/

Breese, P and Burman, W (2005). Readability of notice of privacy forms used by major health care institutions. *Journal of the American Medical Association*. 293: 1593-1594.

Caine, K and Hanania, R (2013). Patients want granular privacy control over health information in electronic medical records. *Journal of the American Medical Informatics Association*. 20: 7-15.

Caine, K and Tierney, WM (2015). Point and counterpoint: patient control of access to data in their electronic health records. *Journal of General Internal Medicine*. 30(Suppl 1): S38-S41.

Cassa, CA, Schmidt, B, et al. (2008). My sister's keeper?: genomic research and the identifiability of siblings. *BMC Medical Genomics*. 1: 32. http://www.biomedcentral.com/1755-8794/1/32

Cheswick, W (2012). Rethinking Passwords. ACM Queue, December, 2012. http://queue.acm.org/detail.cfm?id=2422416

Cimino, JJ (2012). The false security of blind dates: chrononymization's lack of impact on data privacy of laboratory data. *Applied Clinical Informatics*. 3(4): 392-403.

Daemen, J and Rijmen, V (2002). The Design of Rijndael: AES - The Advanced Encryption Standard. Berlin, Germany, Springer-Verlag.

Deleger, L, Molnar, K, et al. (2013). Large-scale evaluation of automated clinical note de-identification and its impact on information extraction. *Journal of the American Medical Informatics Association*. 20: 84-94.
deMontjoye, YA, Radaelli, L, et al. (2014). Unique in the shopping mall: on the reidentifiability of credit card metadata. *Science*. 347: 536-539.
Detmer, DE (2010). Activating a full architectural model: improving health through robust population health records. *Journal of the American Medical Informatics Association*. 17: 367-369.
Dimick, C (2013). Reviewing the new HIPAA rules. *Journal of AHIMA*. 84(3): 40-41.
ElEmam, K, Neri, E, et al. (2007). An evaluation of personal health information remnants in second-hand personal computer disk drives. *Journal of Medical Internet Research*. 9(3): e24. http://www.jmir.org/2007/3/e24/
Ferrández, O, South, BR, et al. (2012). Evaluating current automatic de-identification methods with Veteran's health administration clinical documents. *BMC Medical Research Methodology*. 12: 109. http://www.biomedcentral.com/1471-2288/12/109
Florencio, D, Herley, C, et al. (2007). Do strong web passwords accomplish anything? *Proceedings of the Second USENIX Workshop on Hot Topics in Security (HotSec '07)*, Boston, MA. Usenix http://research.microsoft.com/en-us/um/people/cormac/Papers/hotsec07.pdf
Gostin, LO and Hodge, JG (2002). Personal privacy and common goods: a framework for balancing under the national health information privacy rule. *Minnesota Law Review*. 86: 1439-1479. http://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?article=1086&context=facpub
Gymrek, M, McGuire, AL, et al. (2013). Identifying personal genomes by surname inference. *Science*. 339: 321-324.
Hall, MA and Schulman, KA (2009). Ownership of medical information. *Journal of the American Medical Association*. 301: 1282-1284.
Hanauer, D, Aberdeen, J, et al. (2013). Bootstrapping a de-identification system for narrative patient records: cost-performance tradeoffs. *International Journal of Medical Informatics*. 82: 821-831.
Hardiman, M and Edwards, T (2013). Clarifying the Confusion about HIPAA-Compliant Electronic Communications. Knoxville, TN, PerfectServe. https://www.perfectserve.com/hospital/docs/PerfectServe-Clarifying-Confusion-About-HIPAA-Compliant-Electronic-Communication.pdf
Herley, C, vanOorschot, PC, et al. (2009). Passwords: if we're so smart, why are we still using them? . *Lecture Notes in Computer Science*. 5628: 230-237.
Herzig, TW, Ed. (2010). Information Security in Healthcare - Managing Risk. Chicago, IL, Healthcare Information Management Systems Society.
Hodge, JG, Gostin, LO, et al. (1999). Legal issues concerning electronic health information: privacy, quality, and liability. *Journal of the American Medical Association*. 282: 1466-1471.
Honan, M (2012). Kill the Password: Why a String of Characters Can't Protect Us Anymore. Wired. http://www.wired.com/gadgetlab/2012/11/ff-mat-honan-password-hacker/all/
Houser, SH, Houser, HW, et al. (2007). Assessing the effects of the HIPAA privacy rule on release of patient information by healthcare facilities. *Perspectives in Health Information Management*. 23(4): 1. http://www.pubmedcentral.nih.gov/articlerender.fcgi?pubmedid=18066351
Huesch, MD (2013). Privacy threats when seeking online health information. *JAMA Internal Medicine*. 173: 1838-1839.
Keteyian, A (2010). Digital Photocopiers Loaded With Secrets. CBS News, April 15, 2010. http://www.cbsnews.com/stories/2010/04/19/eveningnews/main6412439.shtml
Kosinski, M, Stillwell, D, et al. (2013). Private traits and attributes are predictable from digital records of human behavior. *Proceedings of the National Academy of Sciences*. 110: 5802-5805.
Levy, S (2014). How the NSA Almost Killed the Internet. Wired, January 7, 2014. http://www.wired.com/threatlevel/2014/01/how-the-us-almost-killed-the-internet/

Libert, T (2015). Privacy implications of health information seeking on the Web. *Communications of the ACM*. 58(3): 68-77.
Liu, V, Musen, MA, et al. (2015). Data breaches of protected health information in the United States. *Journal of the American Medical Association*. 313: 1471-1472.
Lumley, T and Rice, K (2010). Potential for revealing individual-level information in genome-wide association studies. *Journal of the American Medical Association*. 303: 859-860.
Malin, B, Benitez, K, et al. (2011). Never too old for anonymity: a statistical standard for demographic data sharing via the HIPAA Privacy Rule. *Journal of the American Medical Informatics Association*. 18: 3-10.
Malin, B and Sweeney, L (2005). How (not) to protect genomic data privacy in a distributed network: using trail re-identification to evaluate and design anonymity protection systems. *Journal of Biomedical Informatics*. 37: 179-192.
Mandel, J (2015). OAuth2 for Healthcare: Are we ready? SMART Health IT, March 25, 2015. http://smarthealthit.org/2015/03/oauth2-for-healthcare/
McCann, E (2013). Fourth big HIPAA breach for OHSU. Healthcare IT News, July 29, 2013. http://www.healthcareitnews.com/news/fourth-big-hipaa-breach-ohsu
McGee, MK (2013). Google, Amazon Adjust to HIPAA Demands - Cloud Vendors Signing Business Associate Agreements. Healthcare Info Security, October 9, 2013. http://www.healthcareinfosecurity.com/google-amazon-adjust-to-hipaa-demands-a-6133
McGee, MK (2013). HIPAA Breaches in the Cloud - 2 Oregon Incidents Reveal Omnibus Fog. Healthcare Info Security, August 1, 2013. http://www.healthcareinfosecurity.com/hipaa-breaches-in-cloud-a-5959
McGraw, D (2013). Building public trust in uses of Health Insurance Portability and Accountability Act de-identified data. *Journal of the American Medical Informatics Association*. 20: 29-34.
McGraw, D and Hall, JL (2013). FAQ: HIPAA and Cloud Computing (v1.0). Washington, DC, Center for Democracy & Technology. https://www.cdt.org/files/pdfs/FAQ-HIPAAandCloud.pdf
McGuire, AL and Gibbs, RA (2006). No longer de-identified. *Science*. 312: 370-371.
Meystre, SM, Friedlin, FJ, et al. (2010). Automatic de-identification of textual documents in the electronic health record: a review of recent research. *BMC Medical Research Methodology*. 10: 70. http://www.biomedcentral.com/1471-2288/10/70
Norman, D (2009). When Security Gets in the Way. interactions, November/December, 2009. http://interactions.acm.org/content/?p=1308
Pabrai, A (2008). The Single Sign-On Solution. H&HN's Most Wired Magazine, January 23, 2008. http://www.hhnmostwired.com/hhnmostwired_app/jsp/articledisplay.jsp?dcrpath=HHNMOSTWIRED/Article/data/Fall2007/080123MW_Online_Pabrai&domain=HHNMOSTWIRED
Perakslis, ED (2014). Cybersecurity in health care. *New England Journal of Medicine*. 371: 395-397.
Rescorla, A (2001). SSL and TLS: Designing and Building Secure Systems. Reading, MA, Addison-Wesley.
Rindfleisch, TC (1997). Privacy, information technology, and health care. *Communications of the ACM*. 40(8): 93-100.
Rodwin, MA (2009). The case for public ownership of patient data. *Journal of the American Medical Association*. 302: 86-88.
Rothfeder, J (1992). Privacy for Sale: How Computerization Has Made Everyone's Private Life An Open Secret. New York, Simon & Schuster.
Rothstein, MA and Talbott, MK (2006). Compelled disclosure of health information: protecting against the greatest potential threat to privacy. *Journal of the American Medical Association*. 295: 2882-2885.
Rubenfire, A (2015). Hackers breach Anthem; 80M exposed. Modern Healthcare, February 4, 2015. http://www.modernhealthcare.com/article/20150204/NEWS/302049928/hackers-breach-anthem-80m-exposed

Sametinger, J, J Rozenblit, et al. (2015). Security challenges for medical devices. *Communications of the ACM*. 58(4): 74-82.
Sarasohn-Kahn, J (2014). Here's Looking at You: How Personal Health Information Is Being Tracked and Used. Oakland, CA, California Healthcare Foundartion. http://www.chcf.org/publications/2014/07/heres-looking-personal-health-info
Schwartz, PH, Caine, K, et al. (2015). Patient preferences in controlling access to their electronic health records: a prospective cohort study in primary care. *Journal of General Internal Medicine*. 30(Suppl 1): S25-S30.
Stallings, W and Brown, L (2011). Computer Security: Principles and Practice (2nd Edition). Englewood Cliffs, NJ, Prentice-Hall.
Sunyaev, A, Dehling, T, et al. (2014). Availability and quality of mobile health app privacy policies. *Journal of the American Medical Informatics Association*: Epub ahead of print.
Sweeney, L (1997). Guaranteeing anonymity when sharing medical data, the Datafly System. *Proceedings of the 1997 AMIA Annual Fall Symposium*, Nashville, TN. Hanley & Belfus. 51-55.
Sweeney, L (2002). k-anonymity: a model for protecting privacy. *International Journal on Uncertainty, Fuzziness and Knowledge-based Systems*. 10: 557-570.
Sweeney, L, Abu, A, et al. (2013). Identifying participants in the personal genome project by name, Social Science Research Network. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2257732
Tierney, WM, Alpert, SA, et al. (2015). Provider responses to patients controlling access to their electronic health records: a prospective cohort study in primary care. *Journal of General Internal Medicine*. 30(Suppl 1): S31-S37.
Tran, K, Morra, D, et al. (2014). Medical students and personal smartphones in the clinical environment: the impact on confidentiality of personal health information and professionalism. *Journal of Medical Internet Research*. 16(5): e132. http://www.jmir.org/2014/5/e132/
Trotter, F (2012). Who Owns Patient Data? The Health Care Bloy, August 20, 2012. http://thehealthcareblog.com/blog/2012/08/20/who-owns-patient-data/
Vinton, K (2015). Premera Blue Cross Breach May Have Exposed 11 Million Customers' Medical And Financial Data. Forbes, March 17, 2015. http://www.forbes.com/sites/katevinton/2015/03/17/11-million-customers-medical-and-financial-data-may-have-been-exposed-in-premera-blue-cross-breach/
Wagner, R, Allan, A, et al. (2005). Eight Security Practices Offer More Value Than Password Aging. Stamford, CT, Gartner
Wang, CJ and Huang, DJ (2013). The HIPAA conundrum in the era of mobile health and communications. *Journal of the American Medical Association*. 310: 1121-1122.
Wright, A and Sittig, DF (2007). Security threat posed by USB-based personal health records. *Annals of Internal Medicine*. 146: 314-315.