NIH WORKSHOP ON BUILDING A LARGE U.S. RESEARCH COHORT FOR PRECISION MEDICINE RESEARCH

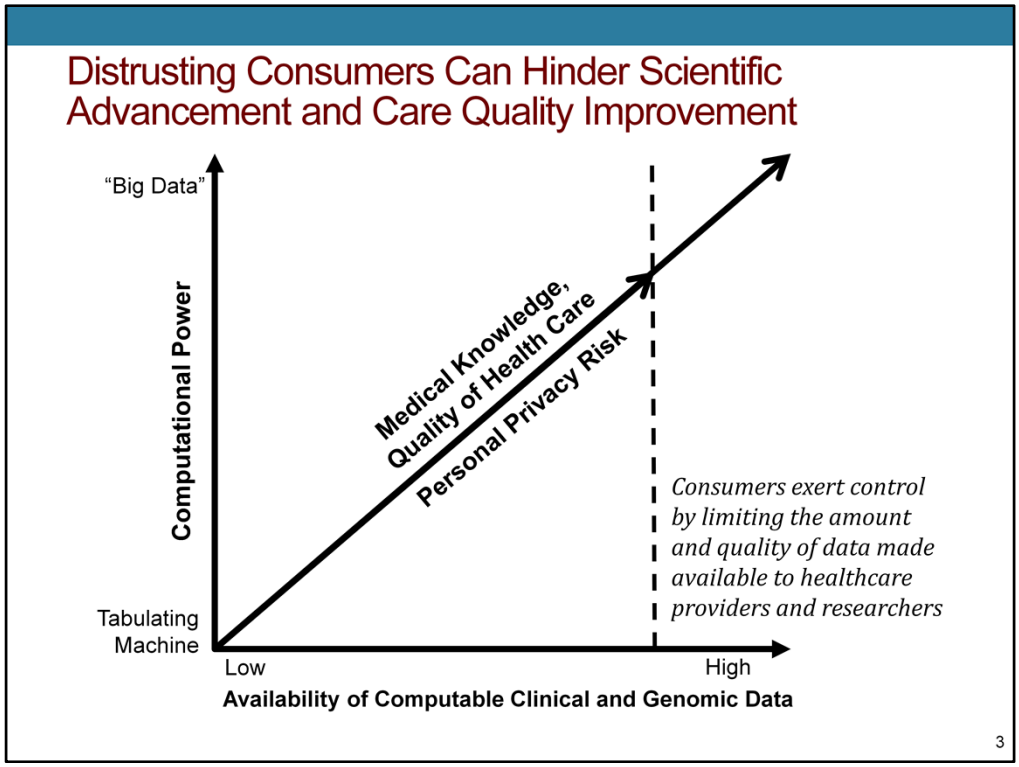
FAIR INFORMATION PRACTICES – BUILDING TRUST WITH CONSUMERS

FEBRUARY 11-12, 2015

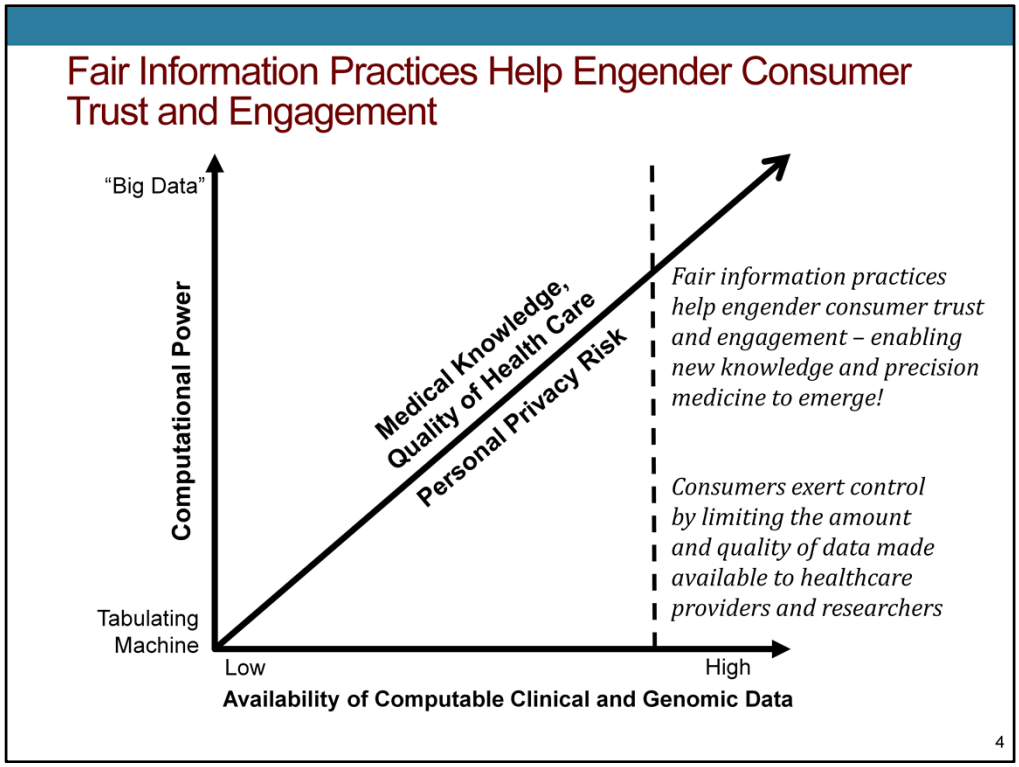
DIXIE B. BAKER, PHD
MARTIN, BLANCK AND ASSOCIATES
DIXIE.BAKER@MARTIN-BLANCK.COM

Building trust with consumers is foundation to the kind of engagement we're seeking for Precision Health. The adoption and adherence to a set of universal principles called "Fair Information Practices," or FIPs, will help establish that trust.

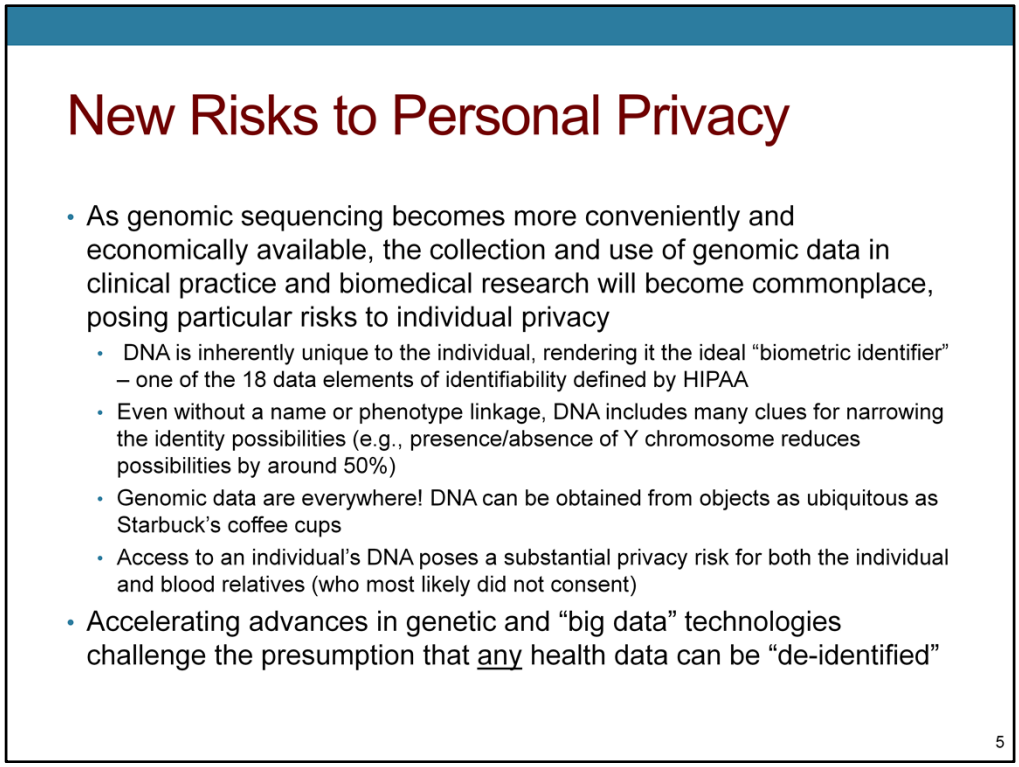
We see evidence of the changing role and perspective of the consumer both in the products and services consumers buy, and in their expectations regarding their own health information.
For example, a high percentage of ...
Smartphone apps and personal sensors are helping consumers take control of their own health. In January of this year, ...
Consumers are purchasing DNA testing services from outside the traditional healthcare system, such as services from 23andMe and Ancestry.com.
As consumers realize that more of their health information is being digitized, the concern over personal privacy is also increasing. **Prospective participants of scientific studies have ranked privacy of sensitive information as one of their top concerns and a major determinant of participation in a study**
But a number of studies have shown that consumers will willingly contribute their data and biological samples to medial research – when their permission is sought. As the UK's National Health Systemdiscovred earlier this year, recently transparency, control, and "no surprises" are key to obtaining consumers' buy-in for use of their health information in biomedical research.



This notional diagram depicts the challenge we face as we capitalize on the availability of massive amounts of computable health data, and our increasing capacity to analyze those data.
On the x-axis, we have the availability of computable clinical and genomic data, and on the y-axis, we have computational power. As more electronic clinical and genomic data about individuals become widely available, and as our computational power continues to explode, we see a real promise of dramatic increases in our medical knowledge and in the quality of healthcare services.
At the same time, we see a concomitant increase in risk to personal privacy.
What tends to happen when consumers realize a risk to their privacy is that they will exert control by limiting the amount and quality of data they make available to healthcare providers and researchers.



The best way to make consumers feel comfortable making their health information available is through adherence to fair information practices, which help engender trust and engagement, enabling new knowledge and precision medicine to emerge!



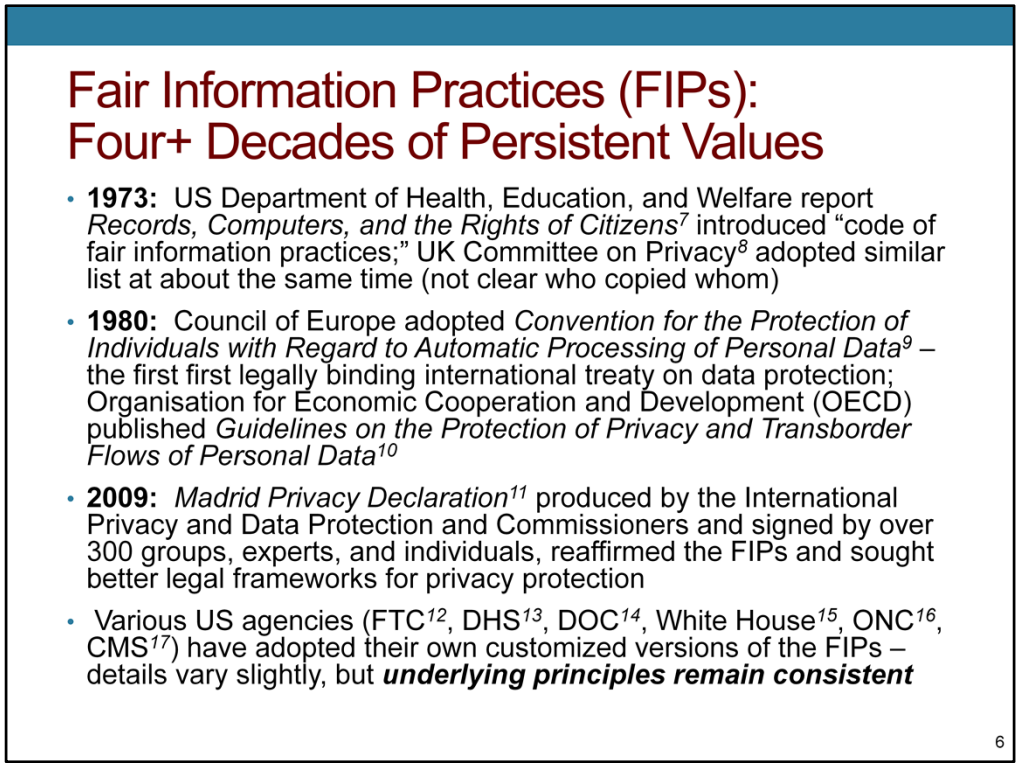
In particular, the challenges posed by the availability of genomic data and "big data" analytics present new risks to personal privacy.

An individual's DNA is unique to that individual, making it an ideal "biometric identifier" – which is one of the 18 identifiers enumerated in the HIPAA Privacy Rule.

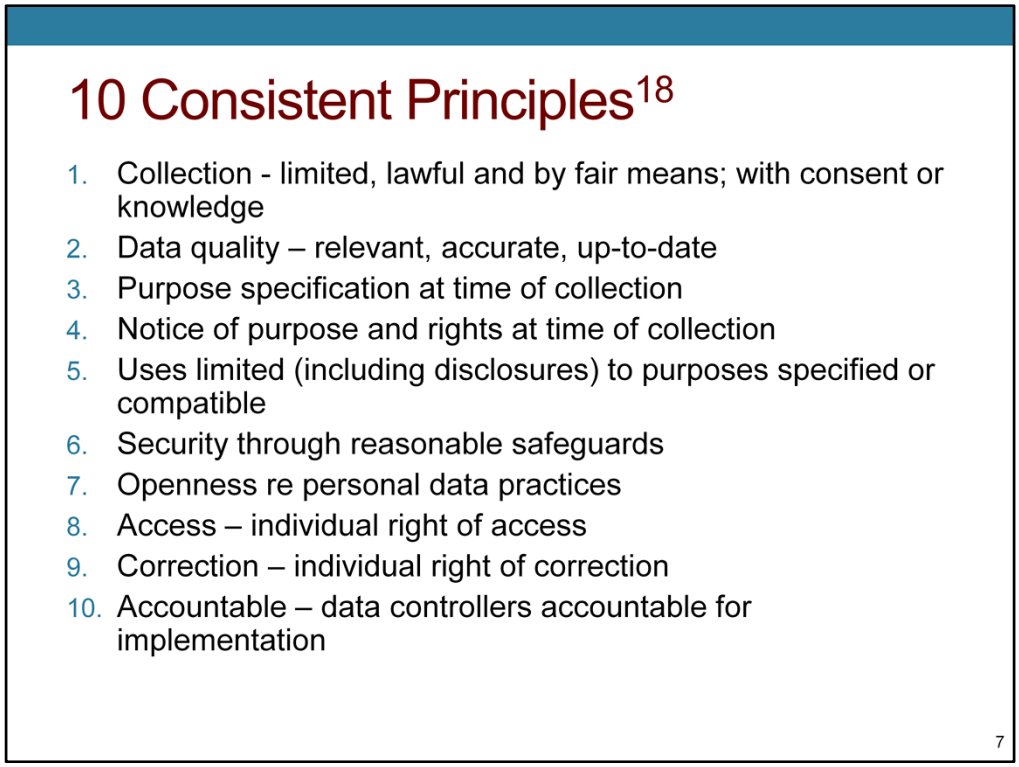
While separating DNA data from identity and phenotype does make it more challenging to associate it with the individual it represents, a genome sequence includes many clues to help narrow down the identity possibilities – for example, the presence or absence of a Y chromosome can reduce the possibilities by about 50%, and coding of visible genetic characteristics and sets of genes commonly associated with heritage can further reduce the possibilities. **Demographic metadata associated with genomic data also is reveling – it's been estimated that the combination of birthdate, sex, and 5-digit zip code can identify ~60% of individuals in the US. (I'm sure that applies to my case.)**

Adding to this privacy risk is the fact that DNA is everywhere! Genomic data can be obtained from things as ubiquitous as Starbuck's coffee cups. And the risk is not only to the individual, but also to the individual's parents, siblings, and children.

Today's "big data" analytic technologies are becoming increasingly expert at mining information from very large volumes of data – leading one to question the Privacy Rule's presumption that any data can be de-identified.



The Fair Information Practices (FIPs) principles have been around for over four decades – and used throughout the world to guide regulatory processes for protecting personal privacy.



In 2012, Graham Greenleaf studied the many instantiations of the FIPs and concluded that these 10 principles are consistent throughout all of them.

Recent US Instantiations

1. The White House. Consumer Privacy Bill of Rights. Appendix A in *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy.* Feb 2012.* [15]
2. HHS Office of the National Coordinator (ONC) *Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information.* Dec 2008.[16]
3. Department of Health and Human Services (HHS). 45 CFR Part 155, Subpart 3. 155.260 Privacy and security of personally identifiable information. Mar 2012.[17]

*Includes appendix comparing Consumer Privacy Bill of Rights with FIPs interpretations by OECD Guidelines, Department of Homeland Security Privacy guidelines, and Asia-Pacific Economic Cooperation (APEC) privacy framework.

8

Recent US Instantiations Compared (1 of 2)

Principle	Consumer Privacy Bill of Rights	ONC Framework	HHS/CMS
Collection	✔ Individual control; Respect for context; Transparency; Focused collection	✔ Individual choice; Collection, use, and disclosure limitation	✔ Individual choice; Collection, use and disclosure limitations
Data Quality	✔ Access and accuracy	✔ Data quality and integrity	✔ Data quality and integrity
Purpose	✔ Focused collection	✔ Individual choice	✔ Individual choice
Notice	✔ Transparency	✔ Openness and transparency	✔ Openness and transparency
Use Limitation	✔ Individual control	✔ Collection, use, and disclosure limitation; Individual choice	✔ Collection, use and disclosure limitations; Individual choice

9

Recent US Instantiations Compared (1 of 2)

Principle	Consumer Privacy Bill of Rights	ONC Framework	HHS/CMS
Security	✔ Security	✔ Safeguards	✔ Safeguards
Openness	✔ Transparency	✔ Openness and transparency	✔ Openness and transparency
Individual Access	✔ Access and accuracy	✔ Individual access	✔ Individual access
Correction	✔ Access and accuracy	✔ Correction	✔ Correction
Accountability	✔ Accountability	✔ Accountability	✔ Accountability

10

FIPs Principles Need to Undergird the Precision Medicine Initiative – Examples

- Communicate using language and media that enable consumers to understand both the benefits and risks of engaging in the Precision Medicine quest
- Values are dynamic! Enable consumers to adjust their sharing preferences, and engage in different ways, over time, as their values and life circumstances change – and as their trust in the enterprise evolves
- Implement best practices in the use of consumer technology:
  - Avoid use of surreptitious technologies to collect information about user behavior for "service improvement" and "customization" purposes without the individual's knowledge and choice
  - Assure that consumer portals and web apps will run on private and safe browser preferences and configurations (e.g., disabled third-party cookies, "don't track me," disabled iframes, White Hat Aviator)
  - Educate consumers on the risks and benefits associated with the use of consumer technologies, and how they can effectively manage those risks for themselves
  - Design apps to minimize exposure and persistence of private information on mobile devices incapable of protecting it
- Avoid surprises!!

11

For More Information

- Robert Gellman has written and maintains a very interesting, detailed history and commentary on FIPs. Check it out at http://bobgellman.com/rg-docs/rg-FIPShistory.pdf

- Contact me @ dixie.baker@martin-blanck.com or 310-791-9671

12

References

1. Tilenius, S. Will an app a day keep the doctor away? The coming health revolution. *Forbes.* 9/8/2013. Available from http://www.forbes.com/sites/ciocentral/2013/09/08/will-an-app-a-day-keep-the-doctor-away-the-coming-health-revolution/ (accessed 2/5/15)
2. Nielson. Hacking health: How consumers use smartphones and wearable tech to track their health. 4/16/2014. Available from http://www.nielsen.com/us/en/insights/news/2014/hacking-health-how-consumers-use-smartphones-and-wearable-tech-to-track-their-health.html (accessed 2/5/15)
3. Patel, V, W Barker, and E Siminerio. *Individuals' Access and Use of their Online Medical Record Nationwide.* Office of the National Coordinator, Department of Health and Human Services. Nov 4, 2014. Available from http://www.healthit.gov/sites/default/files/consumeraccessdatabrief_9_10_14.pdf (accessed 2/5/15)
4. Accenture. 2014 Patient Engagement Survey. May 14, 2014. Available from http://www.accenture.com/SiteCollectionDocuments/PDF/Accenture-2014-Patient-Engagement-Survey.pdf (accessed 2/5/1)
5. Green, R and N Farahany. The FDA is overcautious on consumer genomics. *Nature.* Jan 15, 2014. Available from http://www.nature.com/news/regulation-the-fda-is-overcautious-on-consumer-genomics-1.14527 (accessed 2/5/15)
6. Tarini, BA, et al. Not without my permission: Parents' willingness to permit use of newborn screening samples for research. *Public Health Genomics*. 2009. Available from http://www.cchfreedom.org/pr/tarini_biobanking%20paper_parent%20attitudes.pdf (accessed 2/5/15)
7. US Department of Health, Education, and Welfare. *Records, Computers, and the Rights of Citizens.* 1973. Available from http://www.justice.gov/opcl/docs/rec-com-rights.pdf
8. UK Committee on Privacy. *Report of the Committee on Privacy.* Jan 1973.
9. Council of Europe. *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data.* 1980. Available from http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm (accessed 2/5/15)

References

10. Organisation for Economic Cooperation and Development (OECD). *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.* 1980. Available from http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (accessed 2/5/15)
11. International Privacy and Data Protection and Commissioners. *Madrid Privacy Declaration.* 2009. Available from http://thepublicvoice.org/madrid-declaration/ (accessed 2/5/15)
12. Federal Trade Commission. *Privacy Online: Fair Information Practices in the Electronic Marketplace.* Report to Congress. May 2000. Available from http://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf (accessed 2/5/15)
13. Department of Homeland Security. The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security. Memorandum Number: 2008-01. Dec 2008. Available from http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf (accessed 2/5/15)
14. The White House. Consumer Privacy Bill of Rights. Appendix A in *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy.* Feb 2012.* Available from http://www.whitehouse.gov/sites/default/files/privacy-final.pdf (accessed 2/4/15)
15. Department of Commerce. *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework.* Dec 2010. Available from http://www.commerce.gov/sites/default/files/documents/2010/december/iptf-privacy-green-paper.pdf (accessed 2/5/15)
16. HHS Office of the National Coordinator (ONC) *Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information.* Dec 2008. Available from http://www.healthit.gov/sites/default/files/nationwide-ps-framework-5.pdf (accessed 2/4/15)
17. Department of Health and Human Services (HHS). 45 CFR Part 155, Subpart 3. 155.260 Privacy and security of personally identifiable information. Mar 2012. Available from http://www.gpo.gov/fdsys/pkg/FR-2012-03-27/pdf/2012-6125.pdf (accessed 2/4/15)
18. Greenleaf, G. *The influence of European data privacy standards outside Europe: Implications for Globalisation of Convention 108.* Oct 2011. *International Data Privacy Law*, Vol. 2, Issue 2, 2012. Available from http://ssrn.com/abstract=1960299 (accessed 2/4/15).