If we are to innovate, we must take great care to protect the individual along the way.

As we continue forward in the age of digital information, the risks to personal privacy and security will only continue to increase.

While digital innovation is accelerating progress across the spectrum, it also provides new opportunities for the misuse, malicious actions using, mistakes involving, and inappropriate release of information. With more actions being automatically being taken through the use of artificial intelligence and big data analytics, ensuring proper protocols for the anonymization and thoughtful handling of data is paramount.

We discuss these, and related, information security and privacy risks, legal obligations, and recommendations for addressing these issues.
Co-Founders:

**Michael Welling**, Chair
Partner, Meridian Risk Management

**Joanne Gere**, Executive Director
Westchester Biotech Project

- a borderless initiative
mapping the future
for regional and
international collaboration

On Twitter we’re @WestchesterBio

333 Mamaroneck Avenue, #340, White Plains, New York 10605
917-719-2226  www.WestchesterBiotechProject.org
“We always overestimate the change that will occur in the next two years and underestimate the change that will occur in the next ten.”

Versions attributed to Bill Gates, Arthur C. Clarke, and others
Programs

Roundtables
Roundtable for Researchers
Translating Data Science
Educators and Employers
Building the Biotech Cluster
Government Relations
Intellectual Property
Investors Forum

Symposia
Innovation in Research
Rare Disease Symposium
My First Laboratory

Collaborations
Consortium on Translational Research in the Microbiome
Young Women in Bio/Rutgers Program for High School Seniors
Initiatives

- Westchester Biotech Project Europe
- Westchester Certificate
- Westchester Biotech Blueprint
- Executive in Residence
- Young Investigators
- Expansion Space
Thank You to our Community Partners, Alliance Partners, and Participants!
If we are to innovate, we must take great care to protect the individual along the way.

As we continue forward in the age of digital information, the risks to personal privacy and security will only continue to increase.

While digital innovation is accelerating progress across the spectrum, it also provides new opportunities for the misuse, malicious actions using, mistakes involving, and inappropriate release of information. With more actions being automatically being taken through the use of artificial intelligence and big data analytics, ensuring proper protocols for the anonymization and thoughtful handling of data is paramount.

We discuss these, and related, information security and privacy risks, legal obligations, and recommendations for addressing these issues.
Translating Data Science, Data Ownership and Security

Rebecca Herold
CEO, The Privacy Professor®
Founder, SIMBUS, LLC
FIP, CISSP, CIPP/US, CIPT, CIPM, CISM, CISA, FLMI
Ponemon Institute Fellow

rebeccaгерold@rebeccaHerold.com
A Timely Question…

How can we use health data with the tech of today and tomorrow to bring innovation without data security incidents, and without violating privacy and data ownership?

• How is using data about individuals for research, treatments, etc., similar to the situation with Lacks’ physical cells?
• How is ownership of personal data determined?
• How does ownership of personal data used to produce research results using artificial intelligence (AI), big data analytics, and other tech and algorithms related to privacy, security and data ownership considerations?

In 1951, an African-American woman named Henrietta Lacks was diagnosed with terminal cervical cancer.

For over 60 years Lacks’ cells were commercialized and have generated millions of dollars in profit for the medical researchers who patented her tissue.

Lacks’ family, however, didn’t know the cell cultures existed until more than 20 years after her death.
Important Considerations Are Necessary

• Patient bio-material has been taken without consent and used for research and cures.
• Patient data is also being used to find cures and treatments.
• *What rights do patients have for parts of their own body, and representations, in any form, of their being?*
• *When, where and how is data being taken from, or derived about, individuals?*
• *How is the data being used about them?*
• *What harms could occur to those individuals?*
• *How can associated risks be mitigated and compliance be addresses while supporting innovations?*

Bio-material is considered to be personal information in growing numbers of jurisdictions.
How is data ownership related to privacy?

- Control for how data is collected & derived
- Control for how data is used
- Control over those with whom data is shared
- Ensure data accuracy and integrity
- Accountability to those who violate ownership rights

In addition to the ability of genetic testing to infringe upon the privacy of related individuals, there is also a valid concern that public data may reveal a hidden disease risk that also pertains to a relative who would rather not know. There are many people who know that they may carry a genetic disease and choose not to be tested so that they can continue to live their lives without being defined by a diagnosis. Some also fear that their insurance provider will increase rates if they catch wind of a disease risk (in the US, this is illegal for health insurance providers under the Genetic Information Nondiscrimination Act, but this does not apply to life or disability insurance). This “right to not know” may become threatened when a close relative shares DNA test results that implicate a disease.
Personal Data is Hard to Fully De-Identify

- De-identifying personal data can be undone when combining with other data sets, using AI, big data analytics, etc.
- Tracking use of de-identified data rarely occurs.

Big Privacy: The data privacy compact for the era of big data and AI

Big data and artificial intelligence demand a new privacy compact

Researchers Easily Reidentify Deidentified Patient Records with 95% Accuracy; Privacy Protection of Patient Test Records a Concern for Clinical Laboratories

Oct 10, 2013 | Coding, Billing, and Collections, Compliance, Legal, and Malpractice, Laboratory Management and Operations, Laboratory News, Laboratory Operations, Laboratory Pathology, Laboratory Testing, Management & Operations

Protecting patient privacy is of critical importance, and yet researchers reidentified data using only a few additional data points, casting doubt on the effectiveness of existing federally required data security methods and sharing protocols.

Clinical laboratories and anatomic pathologists know the data generated by their diagnostics and testing services constitute most of a patient’s personal health record (PHR). They also know federal law requires them to secure their patients’ protected health information (PHI) and any threat to the security of that data endangers medical laboratories and healthcare practices as well.

Therefore, recent coverage in The Guardian which reported on how easily so-called “deidentified data” can be reidentified with just a few additional data points should be of particular interest to clinical laboratory and health network managers and stakeholders.

Risky Balance Between Data Sharing and Privacy

In December 2017, University of Melbourne (UM) researchers, Chris Culume, PhD, Benjamin Blumenstein, and Vanessa Tanguy, PhD, published a report with the Cornell University Library detailing how they reidentified data listed in an open dataset of Australian medical billing records.

“We found that patients can be re-identified, without decryption, through a process of..."
Data is Often Not Sufficiently Secured

• Most health industry business leaders will only implement the minimum legally required security & privacy controls…
  – Which leaves most security threats and vulnerabilities unaddressed, and
  – Leaves most privacy issues for research unaddressed.

• Most organizations don’t have full insight or knowledge for where their data is located, which results in lack of security and privacy controls.
Challenge: Data Hides In MANY Locations

- All computing devices that interact with individuals; e.g. from accounting, EHRs, billing, insurance, research, labs, analysis, etc.
- Diagnostic equipment that requires a client profile; e.g. Xray, MRI, ultrasound, etc.
- Personal devices; e.g. pacemakers, insulin pumps, health trackers, personal assistants s/a Alexa, etc.
- Networked devices; e.g. fax machines, copiers, printers, etc.
- BYOD, USB thumb drives, smartphones, tablets, etc.
- Smart wearables; e.g. fitness trackers, smart watches, smart glasses, etc.
- Others: browsers, apps, DVDs, device memory, online, etc.
- Third parties, and their subcontractors, which few organizations have completely documented, etc.
Real Life Case: Data Found on Pacemakers

- Patient data stored on pacemakers purchased on eBay
- Also a history of events stored on the device. Length of history depends on the device.

From DeepSec 2013 Session:
“Research found that 300 medical devices, from 40 different vendors, had hard-coded passwords set.”
- Florian Grunow
When a cell divides, it makes a copy of its DNA. That copy must be verified perfect before the cell will split. Can we say the same about our health data, copied and shared millions of times by hundreds of medical devices, networks and systems?

1. WEARABLES
   - An estimated 500 million people worldwide use fitness wearables.
   - Unauthorized smartphones can connect to unsecured bands and easily transfer unencrypted data without detection.
   - "Total impairment soon" could drive up health insurance rates.

2. SMART CARS
   - Sales of connected auto technologies to triple by 2021, to 153 billion.

3. WIFI TRACKING
   - Frequency lets MIT researchers see humans behind walls.

4. X-RAYS / IMAGING
   - Connected medical imaging market to grow nearly 20 percent by 2020.
   - Patient data transmitted across the web without encryption.

5. BYOD
   - 85% of health organizations allow staff to connect personal devices to the network, putting patient data at risk.

6. DRUG PUMPS
   - More connected medical devices use default login and passwords.
   - Two patients hacked their own pain pumps to kill rivals.

7. IMPLANTS
   - 171 million pacemakers, insulin pumps & other connected devices exist and are vulnerable.

8. SHODAN
   - A search engine just for Internet-connected devices.
   - Rescued 70,000 hacked devices to find "smart" medical devices.

9. RFID CHIPS
   - Microchip implants are already embedded in at least 10,000 employees.

- Over 400 security holes were found in implantable medical devices.
- In healthcare, chips appear to "increase hand-washing compliance."
- Clip data can communicate health data to doctors remotely.

Transmission of data
Unknown data destination
Legal Protections Are Increasing

• US
  – Health Insurance Portability & Accountability Act (HIPAA)
  – Genetic Information Nondiscrimination Act (GINA)
  – US state laws governing health data
  – US state laws governing individuals’ privacy rights
  – Many bills being considered

• International
  – EU GDPR
  – Brazil General Data Protection Law
  – Many other international regulations

• Contractual
HIPAA Privacy Rule Protections

The Privacy Rule protects all "individually identifiable health information" in any form or media, whether electronic, paper, oral, audio, physical, video or other format, with “respect to which there is a reasonable basis to believe the information can be used to identify the individual.”

Think about the data used for research.
What form is it in?
With what data is it combined?
Will research use re-identify individuals?
Where Legal Protections Don’t Exist

- Direct-to-consumer genetic testing businesses
- IOT vendors
- Social media orgs
- Consumer purchased devices
- Mobil device apps
- Other direct to consumer services

The general public are increasingly distrustful of those who want to use their data for research...or ultimately other purposes.

The big picture: What started out as a novelty for genealogists has gone mainstream. There are now more than 50 DNA-testing kit services on the market, estimates Carson Martinez, a health policy fellow at the Future of Privacy Forum.

- MIT Technology Review predicts more than 100 million people may be part of commercial genetic databases within the next two years.
- Amid controversies over internet companies’ collection of personal data, millions are paying to hand over DNA samples to a largely unregulated industry.
- Some worry law enforcement, employers or insurance companies could end up using that DNA information against them.

Driving the news: This month FamilyTreeDNA came under fire for voluntarily giving the FBI routine access to its database of more than 1 million users’ data, allowing agents to test DNA samples from crime scenes against customers’ genetic information to look for family matches.

- FamilyTreeDNA apologized for not disclosing the agreement to consumers. The company told the NYT that users can disable the “matching” option to prevent their data from being visible. Ancestry.com and 23andMe say they require a warrant or subpoena before they consider turning over data to law enforcement.
- It’s not the first time genetic data has been used in cold cases. To catch the Golden State Killer last year, police detectives compared crime scene DNA against publicly available genetic data to identify the suspect.

Drugmakers also want access. Ancestry.com and 23andMe — the largest...
Advice from the FDA & HHS

https://www.youtube.com/watch?v=AmgqX7ITpWg&feature=youtu.be
Consider All Types of Privacy

- Privacy of the Person
- Privacy of Behavior and Actions
- Privacy of Thoughts and Feelings
- Communications Privacy
- Information Privacy
- Territorial Privacy
- Privacy of Association
Privacy Harms

• Loss of self-determination
• Loss of trust
• Discrimination
• Physical harm
• Economic loss
• Reputation damage
• Embarrassment/humiliation
Thoughts to Take Away With You…

• Security controls must be in place throughout the entire lifecycle to ensure data integrity, availability, and confidentiality.
• Privacy issues and risks must be considered and appropriately addressed throughout the entire data lifecycle.
• There is no such thing as 100% security and privacy protections, *BUT* lack of controls provides you with 0% security and privacy protections.
• You ALWAYS need to address more security and privacy beyond regulatory compliance requirements.
• AI, big data analytics, and emerging tech creates new challenges.
• New expectations for data ownership are emerging.
• Third parties bring risks, and often breaches and non-compliance, to those using them.
• Existing and emerging legal requirements will continue.
Questions?

Rebecca Herold
Des Moines, Iowa
Phone 515-491-1564
rebeccaherold@rebeccaherold.com

Web sites:
www.privacyguidance.com
www.SIMBUS360.com

TwitterID: http://twitter.com/PrivacyProf
FIP, CISSP, CIPP/US, CIPT, CIPM, CISM, CISA, FLMI
Ponemon Institute Fellow

Contact Information
Westchester Biotech Project
- a borderless initiative mapping the future for regional and international collaboration

Co-Founders:

Michael Welling, Chair
Partner, Meridian Risk Management

Joanne Gere, Executive Director
Westchester Biotech Project

On Twitter we're @WestchesterBio

333 Mamaroneck Avenue, #340, White Plains, New York 10605
917-719-2226  
www.WestchesterBiotechProject.org