Introduction

• What is “big data”? Modern-day data analytics.

• Data is growing faster than ever before and by the year 2020:
  – every person in the world will create ~1.6 MB data per second
  – digital universe will grow to 44 zettabytes (44 trillion gigabytes)
  – 6.1B+ smartphone users globally

• Cross-Industry Benefits

1. Understand what “big data” means

- **Definition:**
  - Extremely large data sets
  - Analyzed computationally
  - Reveal patterns, trends, and associations (esp. relating to human behavior and interactions)

- **5Vs**
  - Volume
  - Velocity
  - Veracity
  - Variety
  - Value


2. Understand how big data can be leveraged at your organization

- **Big data can reduce US healthcare costs by $300-$450B and improve care**
  - Secondary use of data facilitates medical research

- **White House has invested $200M in big data projects**

- **Strong link between financial performance and effective use of big data across all industries**
  - Analytics to improve products/services and improve marketing
  - 10% increase in data accessibility = $65M+ in additional income for $1000 companies

- **Big data/analytics market to grow from $130B to $203B by 2020**

Sources: [Big data: Lessons from the leaders, Economist Intelligence Unit (The Economist) (2012)](https://www.sas.com/resources/asset/EIU_SAS_BigData_120822.pdf); see also Marr & Ferguson, infra.
3. Understand applicable legal requirements/best practices

- **U.S. privacy laws/enforcement**
  - Federal: HIPAA, FTC Act, FCRA, anti-discrimination laws
  - State: medical privacy, breach notification, information security

- **Health Big Data Recommendations (Fed. Advis. Comm. on Health IT Policy)**
  - address harm/discrimination
  - address uneven policy enforcement (e.g., promote FIPPs for data outside HIPAA)
  - promote robust de-identification methodologies


- **FTC data broker report (2014) and enforcement actions**
  - transparency/consent/choice
  - privacy by design
  - data minimization/disposal
  - avoid discrimination


3. Understand applicable legal requirements/best practices

- **EU data protection principles**
  - Fair/lawful processing (transparency/consent)
  - Purpose limitation
  - Adequate/relevant/not excessive
  - Accuracy
  - Retention (only as long as necessary)
  - Subject rights (right of access/correction)
  - Appropriate technical/organizational measures
  - Not exported unless country ensure adequate level of protection

- **UK ICO report: Big data, artificial intelligence, machine learning and data protection (2017)**
  - Fairness/transparency
  - Consent/legitimate interest
  - Purpose limitation
  - Information security
  - Anonymization

- **EDPS Opinion 7/2015: “Meeting the challenges of big data”**
  - Transparency
  - User control
  - Protection by design
  - Accountability
4. Be mindful of the FCRA and discriminatory practices

- FTC Act Section 5 (unfair/deceptive acts)
  - consent and privacy misrepresentations
  - data security of databases
- FCRA
  - applies to consumer reporting agencies (CRAs), credit bureaus, and employment screening companies, but can be broader (e.g., data brokers)
  - governs consumer reports used to determine eligibility for credit, employment, insurance, and housing
  - example: company makes credit decisions based on consumer’s zip codes, which impacts particular ethnic groups


5. Privacy By Design and Privacy Impact Assessments

- Privacy/security embedded proactively when system/practice designed
- Privacy/transparency embedded into all lifestyles stages
  - Privacy by design and simplified consumer choice/transparency
- EU General Data Protection Regulation (May 2018)
  - Article 25 (Data protection by design and by default)
  - Article 35 (Data protection impact assessment)

6. Anonymize Data

- **HIPAA De-identification Standard**
  - Safe Harbor Method
  - Expert Determination Method

- **EU anonymization**
  - Opinion 05/2014 on “Anonymisation Techniques (WP216)"

- **NIST Standard**
  - Suppression
  - Averaging
  - Generalization
  - Perturbation
  - Swapping

7. Conduct Vendor Diligence

- Review vendors practices for compliance with laws and best practices (e.g., consent/notice, security, etc.)
- Conduct security assessment of vendor
- Identify sub-vendors/data sources
- Implement strong contractual language (e.g., reps/warranties on data and data collection)


8. Ensure robust information security

- Anonymization/pseudonymization
- Data minimization
- Access/account controls
- Ensure secure infrastructure
  - infrastructure security/secure computations
  - granular access controls/audits
  - secure data storage/logging
  - end-point validation and filtering
- Encryption in transit (and at rest)
- Secure data disposal

9. Enable International Data Transfers

- Privacy Shield adopted July 2016
- Other legal EU data export mechanisms:
  - Model Clauses/Standard Contractual Clauses (“SCCs”)
  - Binding Corporate Rules (BCRs)
  - Consent (limited circumstances)


10. Know (and Own) Your IP Rights

- Vendor insists on “owning” data and algorithms that they shouldn’t
  - new land grab for rights to new or enhanced algorithms
- In data analytics and IoT, information is collected and pulled in many more directions than before and involves more parties
  - mapping now must also track the rights and obligations of each involved party
- Derived information should also be addressed (i.e., times and location of use, behavior patterns) and other new purposes
Big Data and Secondary Uses of Data: Practical Tips to Avoid Privacy Pitfalls and Regulatory Risk

QUESTIONS?

Corey M. Dennis, CIPP/US
Director of Privacy & Counsel
Pharmaceutical Product Development, LLC (PPD)
corey.dennis@ppdi.com

Asra Ali, MS, CHC, CHPC, CIPM
Compliance and Risk Manager
Healthscape Advisors
aali@healthscape.com