HIPAA Summit 22

Afternoon Plenary – Welcome!
HIPAA, HITECH and Health Reform

February 6, 2014

Agenda 1

- 1:00 PM - Health Reform: Why We Are Here
  - **Bill Braithwaite**, MD, PhD (Co-Chair)
- 1:15 PM - ONC Privacy and Security Policy Update
  - **Joy Pritts**, Esq., Chief Privacy Officer of ONC
- 1:45 PM – The Perspective of a Privacy Advocate
  - **Deven McGraw**, Director, Health Privacy Project of CDT
- 2:15 PM - HIPAA and Payment and Delivery System Reform
  - **Paul Smith**, Esq., Partner of Hooper, Lundy & Bookman
- 2:45 PM – Outsourcing IT Under BAA: Assuring Security
  - **Chris Davis**, Sr. Solutions Architect of Verizon
- 3:15 PM - Break

Agenda 2

- 3:45 PM Health Insurance Exchange Privacy and Security Issues
  - **Elizabeth Ferrell**, Esq., Partner of McKenna, Long & Aldridge
- 4:15 PM Technical Security Challenges in MU Incentives
  - **Margret Amatayakul**, MBA, President of Margret\A Consulting
- 4:45 PM Managing Mobile Device Security under HITECH
  - **Kathy Downing**, MA, Director, Practice Excellence of AHIMA
- 5:15 PM **Adjournment**

Health Reform:
Why We Are Here

William R. “Bill” Braithwaite, MD, PhD, FACMI, FHL7
AKA “Dr. HIPAA”

February 6, 2014

1996 HIPAA 1.0 – Administrative Simplification

- Improve the efficiency and effectiveness of the health care system by standardizing the electronic data interchange of certain administrative and financial transactions.

- Protect the security and privacy of transmitted information.

HIPAA
Health Insurance Portability
and Accountability Act

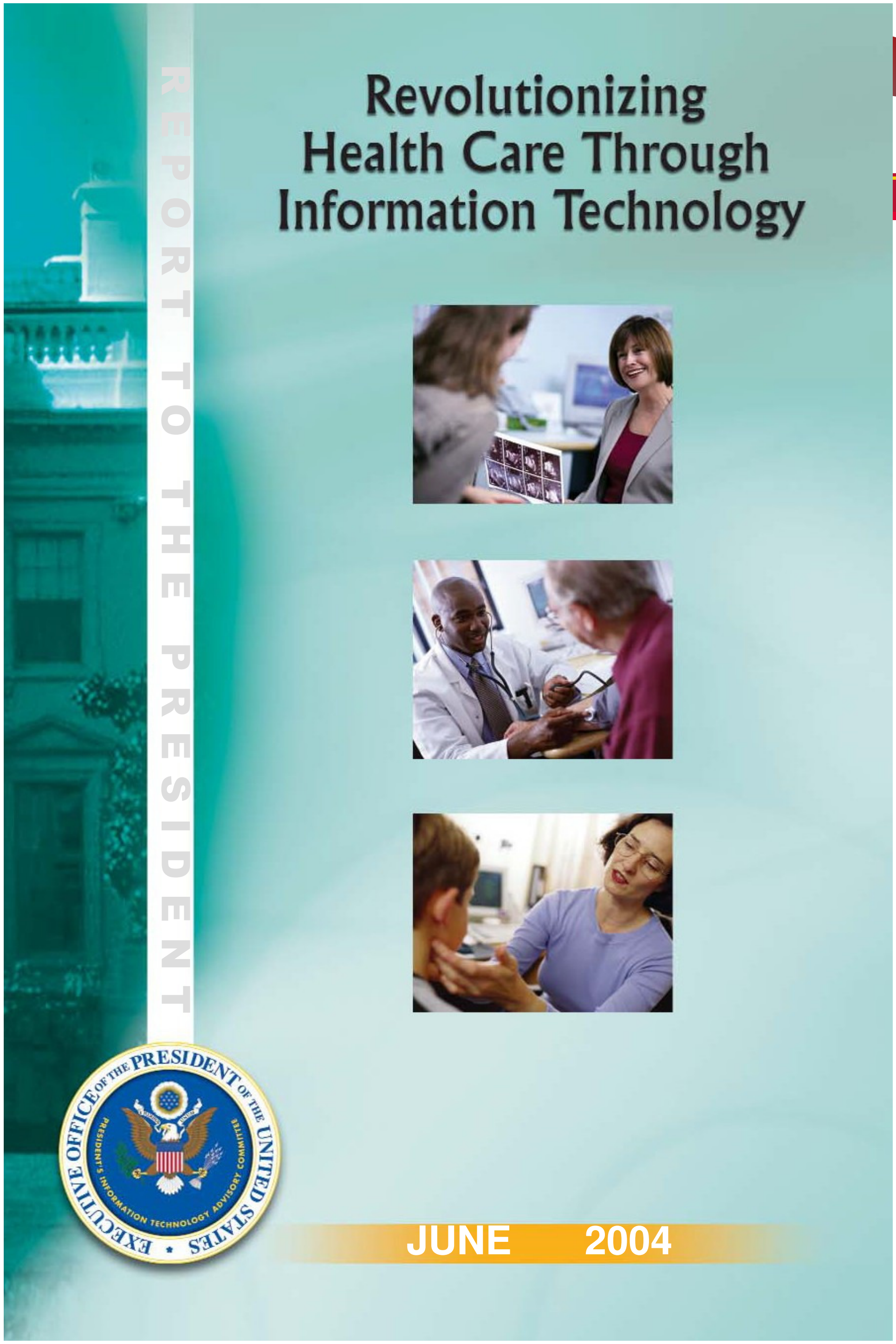
Title II - Subtitle F – Administrative Simplification

HIPAA 1.0 Intent (in English)

- Any two healthcare entities can conduct routine interactions rapidly and entirely electronically using standardized identifiers, transactions, and code sets.
- Telephone, fax, or paper interactions are needed rarely.
- Any entity incapable of doing this themselves can participate cost-effectively using a clearinghouse.
- Savings of time and hassle are significant.
- Privacy and security of patient information is assured.

- Industry representatives expected full implementation within two years…

2004 PITAC



REPORT TO THE PRESIDENT

Revolutionizing Health Care Through Information Technology

EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES

PRESIDENT'S INFORMATION TECHNOLOGY ADVISORY COMMITTEE

JUNE 2004

…the potential of IT to improve the delivery of care while reducing costs is enormous…

2009 HIPAA 2.0 – American Recovery and Reinvestment Act (ARRA)

- Title XIII: Health Information Technology for Economic and Clinical Health Act (HITECH)
- Business Associates are now DIRECTLY subject to the HIPAA Security Rule, including new classes of entities
- Office of the National Coordinator of HIT
- Incentive Funding
- Privacy and Security
  - Refinements
  - Breach Responses
  - Increased Enforcement

- Plus Migration to ICD-10-CM/PCS

2010 HIPAA 3.0 – Patient Protection and Affordable Care Act (ACA)

- SEC. 1104. ADMINISTRATIVE SIMPLIFICATION
- Transaction Standard Refinements
  - Operating Rules
  - Electronic Funds Transfer
- Health Plan Certification
- Increased Enforcement

2013 HIPAA's Got Teeth! – The Omnibus Rule …

Why Do We Care About HIT?

- from 1999 IOM Report: To Err is Human

- Avoidance of medical errors.
  - Up to 98,000 avoidable annual hospital deaths due to medical errors.
- Avoidance of healthcare waste.
  - Up to $300B spent annually on treatments with no health yield.
- Acceleration of health knowledge diffusion.
  - 17 years for medical evidence to be integrated into practice.
- Reduction of variability in healthcare delivery and access.
  - Access to specialty care is highly dependent on geography.
- Empowerment of consumer involvement in health management.
  - Patients minimally involved in own health decisions.
- Strengthening of health data privacy and protection.
  - Public fear of identity theft and loss of privacy.
- Promotion of public health and preparedness.
  - Surveillance is fragmented, and untimely.

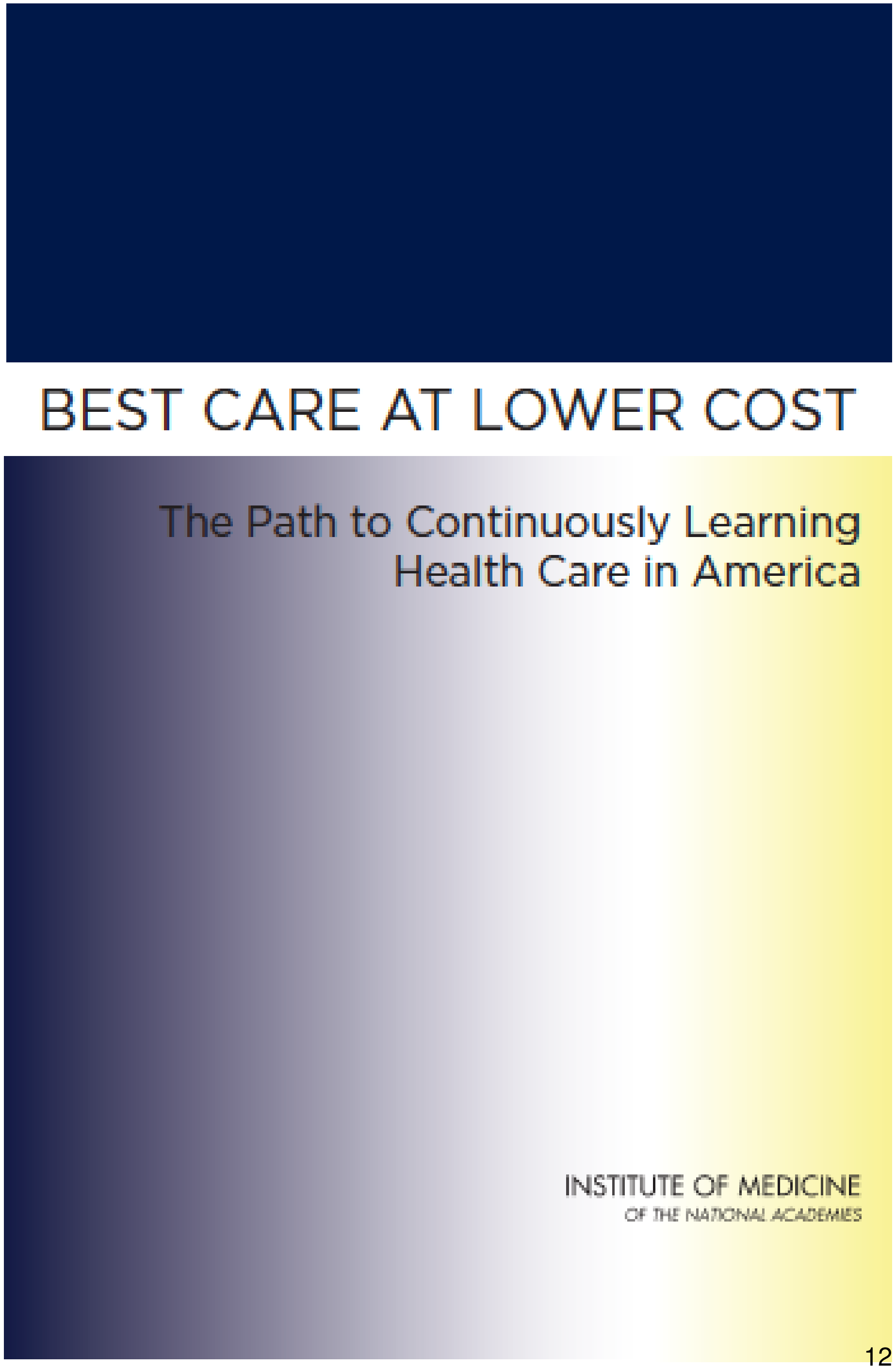
Paper records cannot solve these problems!!!

2012 IOM Report

"The Best Care at Lower Cost: The Path to Continuously Learning Health Care in America"

- Report offers findings, conclusions, and recommendations for implementation by key stakeholders to achieve a health care system that is consistently reliable and that constantly, systematically, and seamlessly improves.

- $765B excess costs annually



BEST CARE AT LOWER COST

The Path to Continuously Learning
Health Care in America

INSTITUTE OF MEDICINE
OF THE NATIONAL ACADEMIES

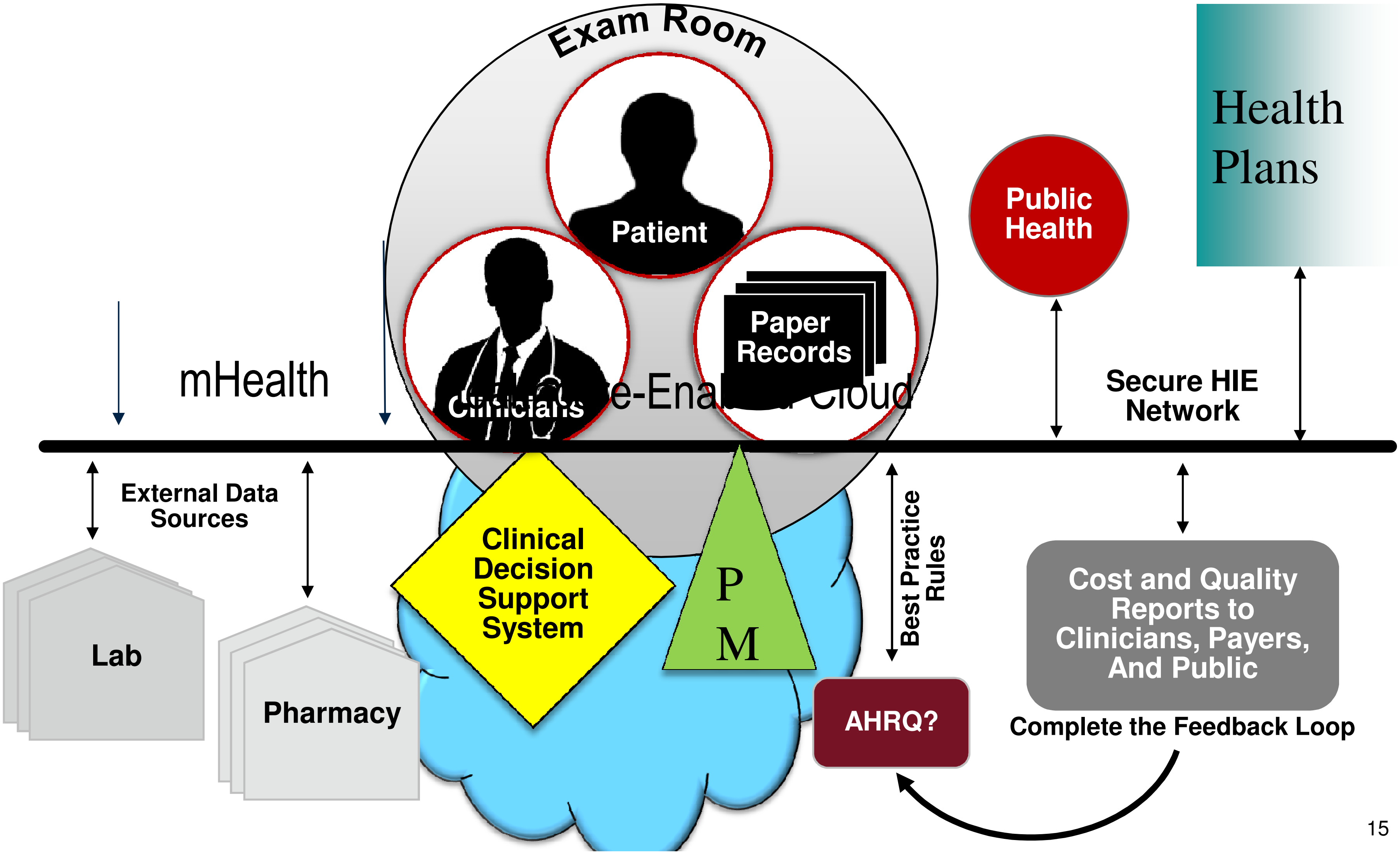
If Other Industries Operated Like Healthcare:

- **Banking**: automated teller machine (ATM) transactions would take days or longer as a result of unavailable or misplaced records.
- **Home Building**: carpenters, electricians, and plumbers each would work with different blueprints, with very little coordination.
- **Shopping**: product prices would not be posted, and the price would vary widely within the same store, depending on the source of payment.
- **Automobile Manufacturing**: warranties for cars would not exist so few factories would seek to monitor and improve production line performance and product quality.
- **Airline Travel**: each pilot would be free to design his or her own preflight safety check, or not to perform one at all. On average one jet would crash each day and cause no changes to the system.

Standard Best Practices from Other Industries:

- **Records** are immediately updated and available for use by patients;
- **Care** has been proven reliable at the core and tailored at the margins;
- **Needs and Preferences** of Patient and Family are a central part of the decision process;
- All team members are **fully informed** in real time about each other's activities;
- Prices and total costs are **fully transparent** to all participants;
- **Incentives** are structured to reward outcomes and value, not volume;
- **Errors** are promptly identified and corrected; and
- **Results** are routinely captured and used for continuous improvement.

Evolution of the Healthcare Paradigm



Future for Healthcare

- **Goal**: Best Care at Lower Cost (2012 IOM Report)
- **Means**: Clinician/Patient direct interaction with Clinical Decision Support System (CDSS) ("Meaningful Use").
- **Drivers**: HIE + EHR + CDSS => SAVES LIVES and $$$
  - Interoperable HIE is KEY to Meaningful Use of HIT which, in turn, is KEY to a continuously learning healthcare system!
- **Requires**: EHR (with CDSS and HIE) and:
  - Interoperability with sources of administrative data, clinical data, and computable rules for best clinical practices (Standards).
  - Incentives to incorporate into healthcare practice (Resources and Regulations).
  - Investigations of systemic failures to enable systems that detect and prevent errors through best practices at the point of decision making (Research).
  - Trust through interoperable security and privacy (including patient consent).

Motivation …

“Knowing is not enough; we must apply.
Willing is not enough; we must do.”

Johann Wolfgang von Goethe, circa 1820

"If you cannot measure it, you cannot improve it.“

Lord Kelvin, circa 1853

“Illigitimi non carborundum!”

Anonymous, circa 1938

Questions?

Bill at Braithwaites dot com

HIPAA Privacy Rule of Thumb

- **Don’t surprise** the patient with a use or disclosure they don’t expect!
  - Tell the patient about uses and disclosures necessarily part of normal operations of the healthcare enterprise (NPP of TPO).
    - No consent required.
  - Give the patient the opportunity to object to limited disclosures in common practice.
    - e.g., name in hospital directory.
  - Follow required procedures for public policy exceptions.
    - e.g., required reporting of contagious disease.
  - Get explicit permission for anything else.
    - e.g., signed authorization
- **Don’t forget**: Terms “Reasonable and Appropriate” were used 365 times in the 365 page Privacy Rule.

HIPAA Security Rule of Thumb

- Identify & assess risks/threats to electronic information:
  - Availability
  - Integrity
  - Confidentiality
- Assess risk
- Manage risk
  - Implement appropriate and reasonable administrative, physical, and technical security safeguards.
  - Consider size, complexity, technical infrastructure, hardware, and software security capabilities, costs, and the probability and criticality of potential risks.
- Educate/Train
- Document and Monitor
- Repeat cycle periodically …

- Terms “reasonable and appropriate” used 75 times in 75 page Rule!

Privacy and Security Reflections from Dr. HIPAA

- Design Privacy and Security into the Health IT System.
  - Build it right into the infrastructure, don’t try to tack it on afterwards.
- Find and Manage Risk in Reasonable and Appropriate ways.
  - Earthquake Preparations in San Francisco vs DC?
- People are Fallible – so is any System built by People.
  - Design for Failure.
- People are Creative – and can always find a way around any control.
  - Trust, but Verify – Analyze those Audit Trails!
- Educate; Don’t just Train.
  - People follow intent of instruction better when they understand why!
- Use Common Sense – Think First, Learn from Others.
  - Encrypt all portable media, but don’t set the password complexity and refresh requirements so high that people must write their passwords down and carry them in the same bag as the device.