Privacy and Security – A US Perspective

Innovations to enhance research

Kevin Peterson, MD MPH FRCS(Ed) FAAFP

Professor and Director
Center of Excellence in Primary Care
University of Minnesota Medical School
Minnesota, USA

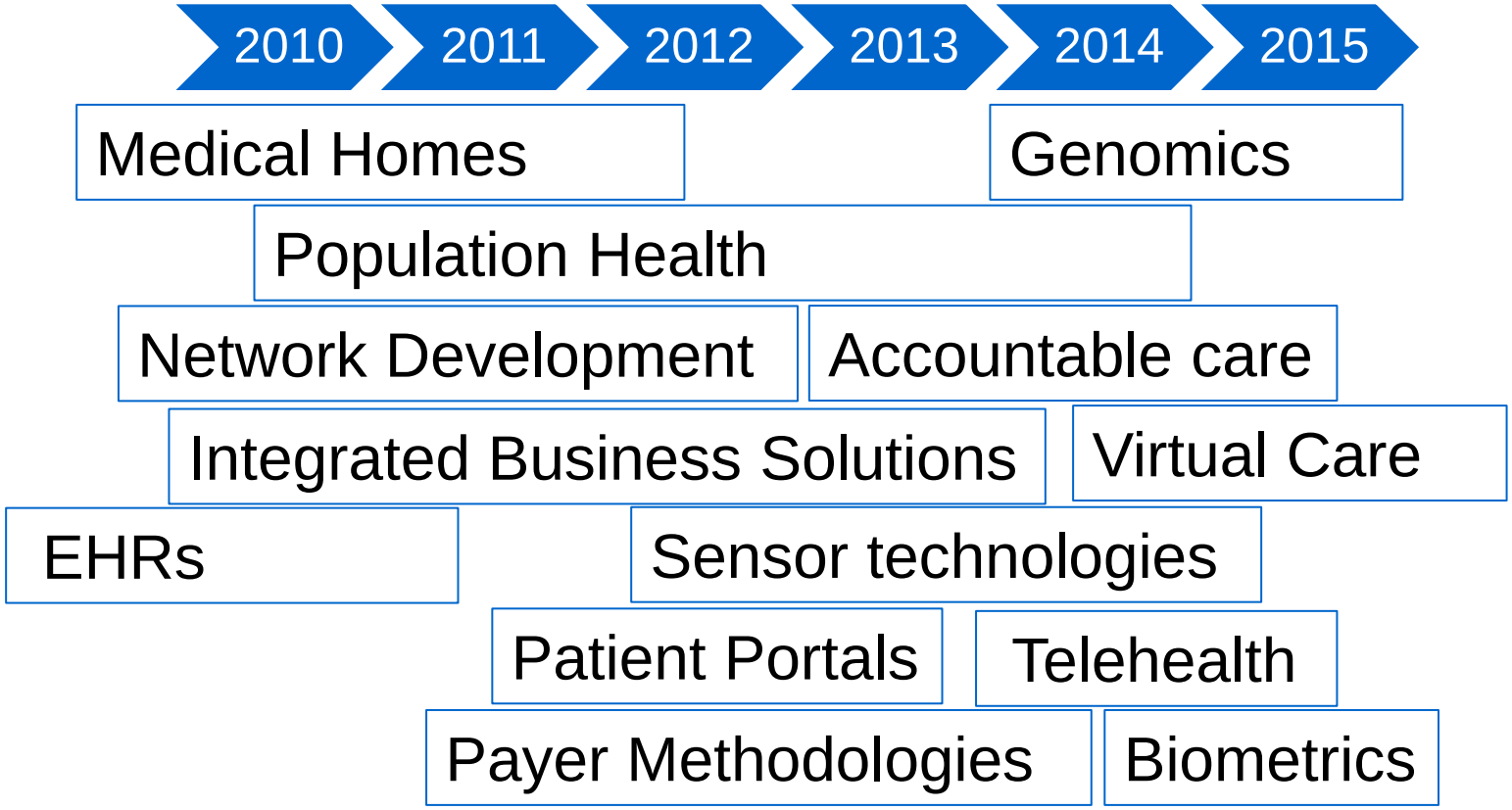
A Brief History of US Privacy

- English common law-
  - freedom from ‘physical interference of life and property’
  - US Constitution – ‘life, liberty, and the pursuit of happiness’
    - privacy was initially conceived of as an extension of life/property rights
- New chapters in privacy
  - Newspapers (1850) and cameras (1880) led to the new definition
  - The Right to Privacy
    - Warren,Brandeis, Harvard Law Review, 1890
    - Extension of implied trust in society
      - Limitation of the extent of public dissemination
  - Introduction of electronic health records (1980)

Evolving Care Models

Volume ⟺ **Value**

Fee-for-service Shared savings Episode Payment Partial Capitation Global Payments



HIPAA

- **Health Insurance Portability and Accountability Act (HIPAA)**

Title II: Administrative Simplification provisions. Established national standards for electronic health care

  - 2.1 Privacy Rule
  - 2.2 Transactions and Code Sets Rule
  - 2.3 Security Rule
  - 2.4 National Provider Identifier
  - 2.5 Enforcement Rule

Privacy rule

- Regulates the use and disclosure of Protected Health Information (PHI) held by "covered entities"
  - Updated in 2013 (Final Omnibus Rule Update) to include all Business Associates of covered entities
- Defines PHI
  - any information which concerns health status, provision of health care, or payment for health care that can be linked to an individual
- Exceptions
  - Law enforcement
  - To facilitate treatment, payment, or health care operations

Security Rule

Specifically addressed Electronic PHI

- Defines three classes of security safeguards
  - administrative, physical, and technical
- Required and addressable specifications
  - mandatory versus recommended
- Provided a minimum standard
  - responsibility falls on covered entities to take all reasonable precautions
  - many different interpretations

HITECH Act

- Health Information Technology for Economic and Clinical Health
  - Title XIII of the American Recovery and Reinvestment Act (Obamacare)
- Privacy rule extended HIPAA
  - data breaches which affect 500 or more persons must be reported to:
    1. US Department of Health and Human Services
    2. The news media
    3. People affected by the data breaches
  - updated civil and criminal penalties
  - broadens who can access records

Privacy is state based

- 10 States have a ‘right to privacy’ in their constitution
  - 46 states protect HIV information
  - 41 have a cancer registry
  - 38 States protect genetic information

The potential impact of data sharing in healthcare could amount to $300-$450 billion in annual value

Identifiability vs. anonymity

- Potential concerns of re-identification
  - 1997 –identified Gov. Welds health information from anonymous Massachusetts health insurance claims
    - (Barth Jones, 2012)
  - 2013 Researchers successfully identified male genomes through correlation with commercial geneaology databases
    - (Gymrek et al, Science, 2013)
- Office of the National Coordinator evaluations
  - ‘Safe Harbor’ from 0.01% to 0.25% of population
  - Limited Datasets from 10% to 60%

2015 – The year of the hack

- From 2009 – 2014
  - 120 million people had health data compromised
- 2015 (First three months)
  - 91 million more
  - Sophisticated attacks
  - Suspected to originate from China
  - Underground value of $20 per record

Health Information Exchange (HIE) in Minnesota

HIE is often vendor specific.

- Clinics with HIE 75%
- Clinics with HIE to unaffiliated partners* 40%
- Hospital HIE with other providers 73%
- Hospitals HIE with unaffiliated partners* 40%
- Nursing homes HIE 38%

In view of history and the legal obstacles, achieving a social contract (ex. GoDarts) with the people and/or US legislature appears unlikely

** Providers with a different medical record vendor*

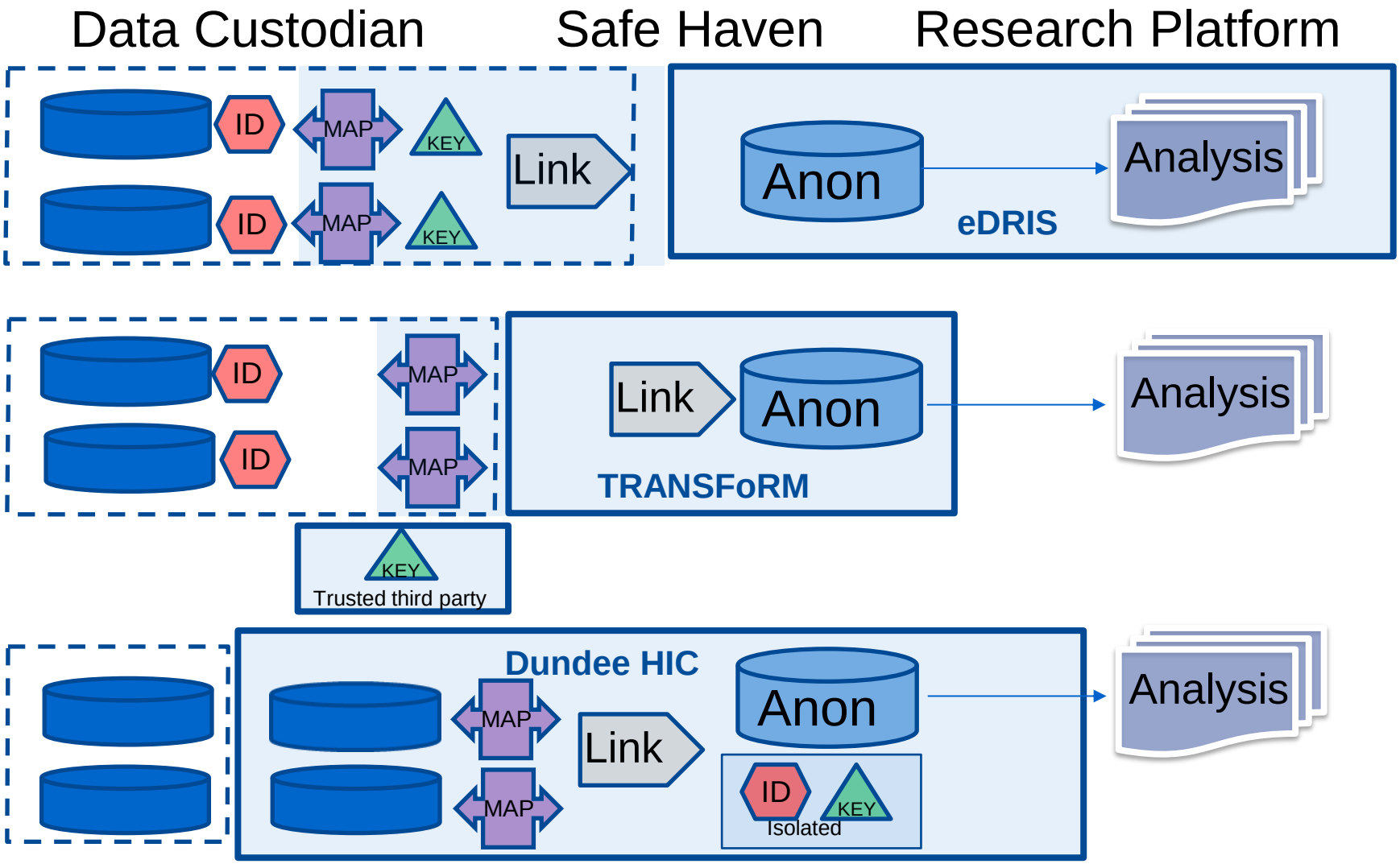
New approaches to privacy

Security requires well-documented standards and tools

- Zone Models - Standardised data privacy frameworks[1]
  - Provides a framework for discussing and creating privacy compliant data flow
- Engagement of advocacy organizations
  - Privateaccess Inc.
  - Providing the ability for authenticated providers to search for personal information based on “private access” rights that each individual creates.[2]

1. *Kuchinke W, Ohmann C, et al. Int J Med Inform [Internet]. Elsevier Ireland Ltd; 2014;83(12):941–57.*
2. *https://www.privateaccess.info/)*

Pseudo-anonomyzing data

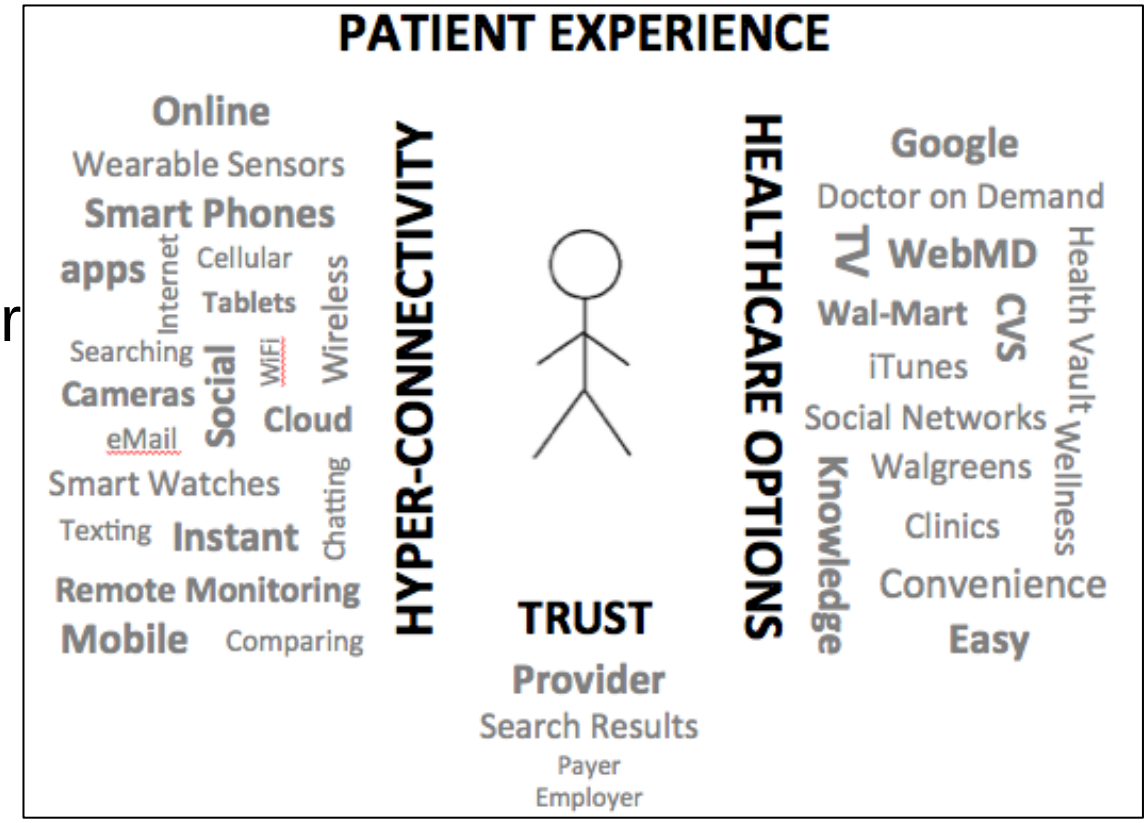


Patients – An Underutilized Resource

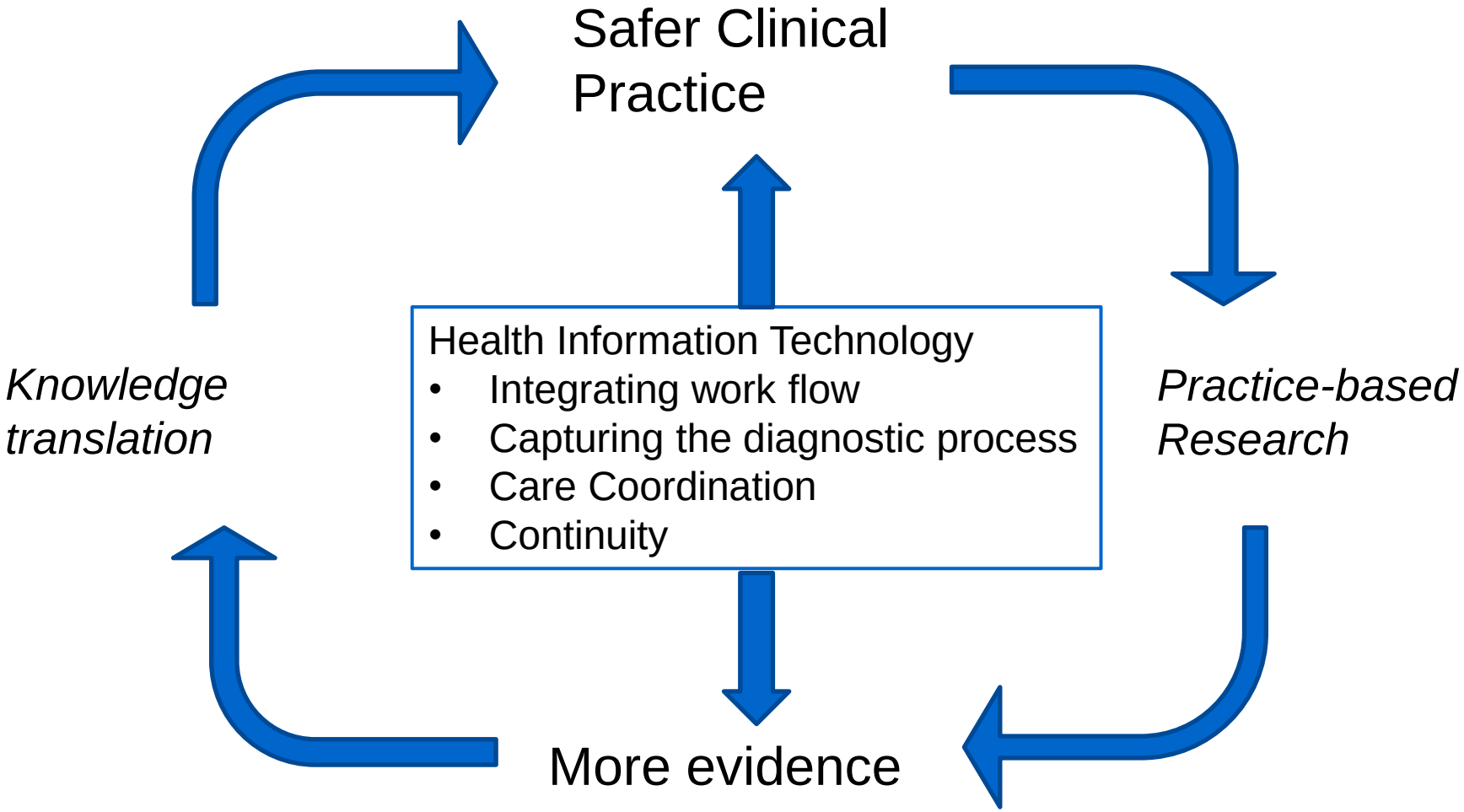
- Greatest interest in the most intimate details of the record
- **I**mprove the relevance of the research question
- Increases the effectiveness with which research findings can be translated back to the community.

Increasing Consumer Awareness

- A less tolerant "consumer" of healthcare
- More willing to consider options
- Providers are still the most trusted advisors
- What happens when systems fall behind?



IOMs Learning Health Care System



IOM (Institute of Medicine), Digital Infrastructure for the Learning Health System : The Foundation for Continuous Improvement in Health and Health Care 2011.

Community Engaged and Practice Based

Center of Excellence in Primary Care- Clinical research conducted in the settings where the US population most commonly receives care

150 Primary Care Practice-Based Research Networks

- 73,000 Network Members
- 17,000 Primary Care Practices
- Serving 52.7 Million People