



Guiding Principles for Data Access and Sharing: What protections are needed?

February 12, 2015

**David H. Ledbetter, Ph.D.
Geisinger Health System**

dhledbetter@geisinger.edu

What protections are needed?

“The EHR workgroup does not believe that any new or unique cybersecurity measures will need to be developed specifically for the project, but adoption of **industry-wide best practices and technologies, and ongoing vigilance will be essential to establishing and maintaining trust of study participants and that of collaborating organizations”.**

What protections are needed?

- **Which best practices?**
 - **Clinical vs. research**
 - **Other private sector industries**
 - **U.S. vs. International standards**
 - **Whichever represents highest standard**
- **Training/education requirements for all individuals with access to data**
- **Monitoring/audit procedures**
- **Consequences of data breach or misuse.**

Fair Information Practices (FIPs):10

Consistent Principles¹⁸

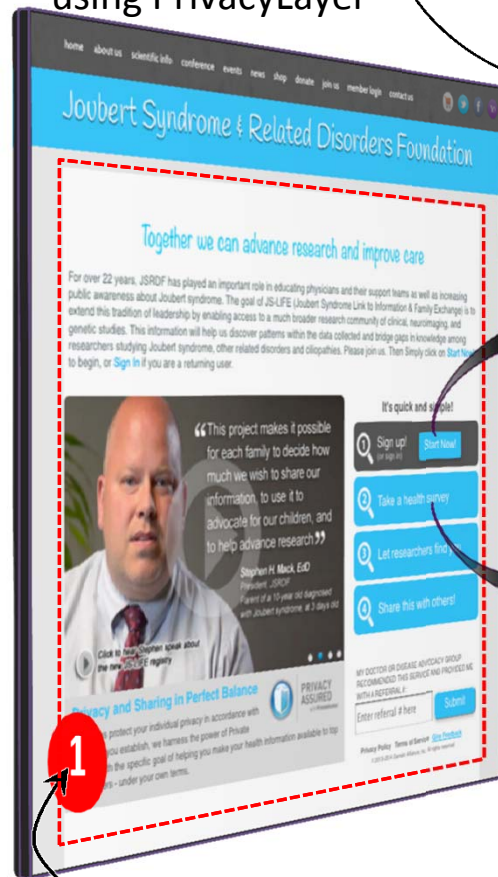
1. Collection - limited, lawful and by fair means; with consent or knowledge
2. Data quality – relevant, accurate, up-to-date
3. Purpose specification at time of collection
4. Notice of purpose and rights at time of collection
5. Uses limited (including disclosures) to purposes specified or compatible
6. Security through reasonable safeguards
7. Openness re personal data practices
8. Access – individual right of access
9. Correction – individual right of correction
10. Accountable – data controllers accountable for implementation

From Dixie Baker, Ph.D.

PEER: Creating an environment of trust (from Sharon Terry)

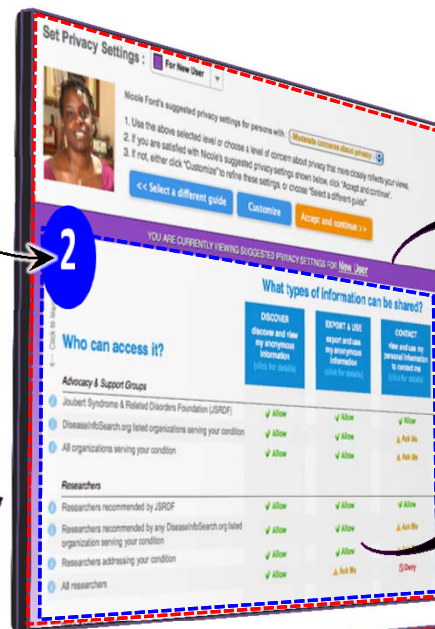
Privacy Set Up:

Individual registers and sets privacy preferences using PrivacyLayer®



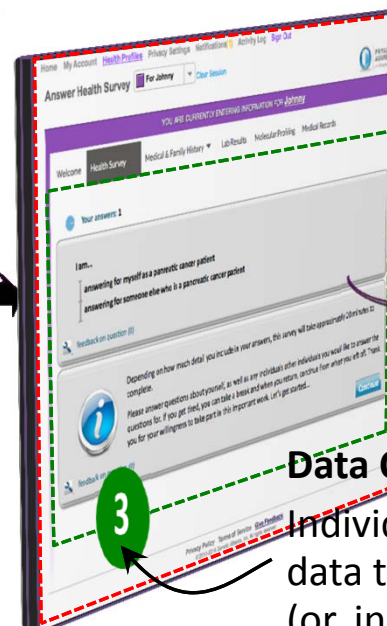
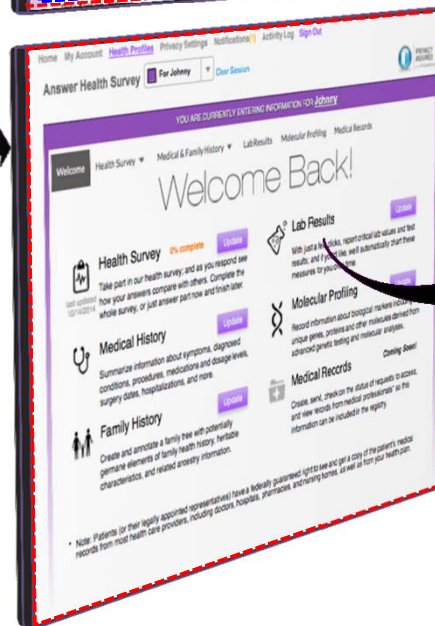
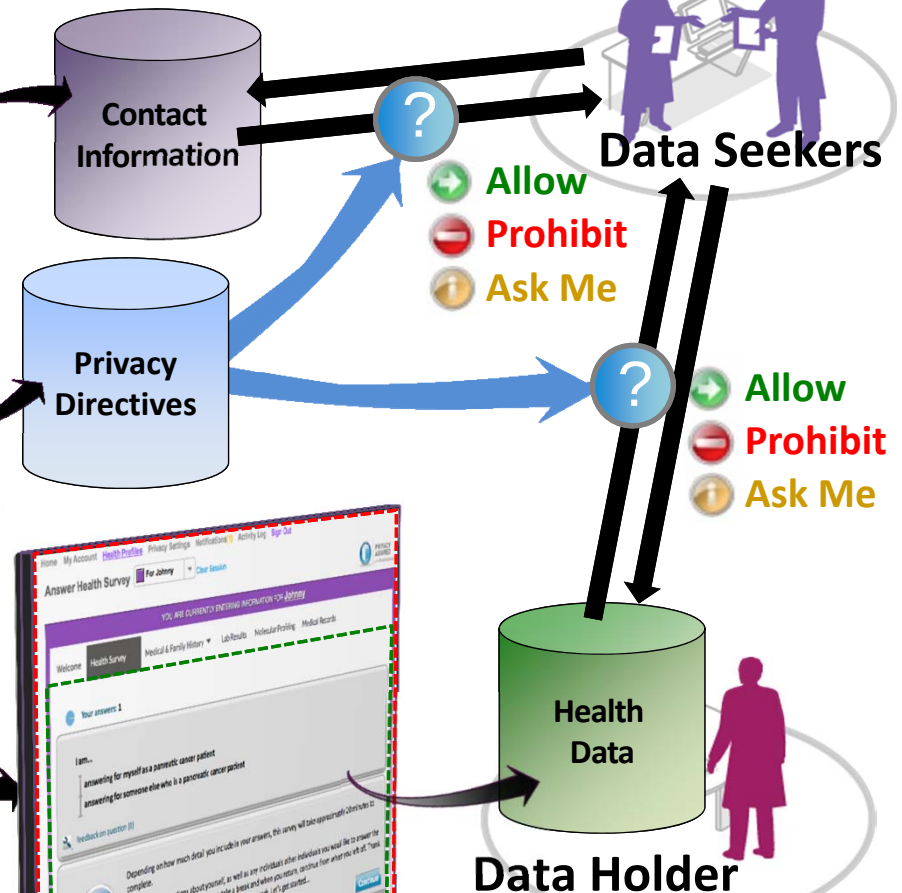
Set-up:

Trusted organization simply embeds a PEER entry point into its website



Data Access:

Data Seekers access health data and contact information, as authorized

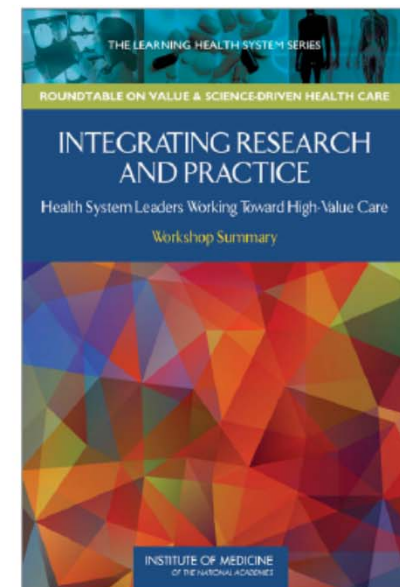


Data Capture (or Order):

Individual provides health data through survey questions (or, in future, from their EHR)

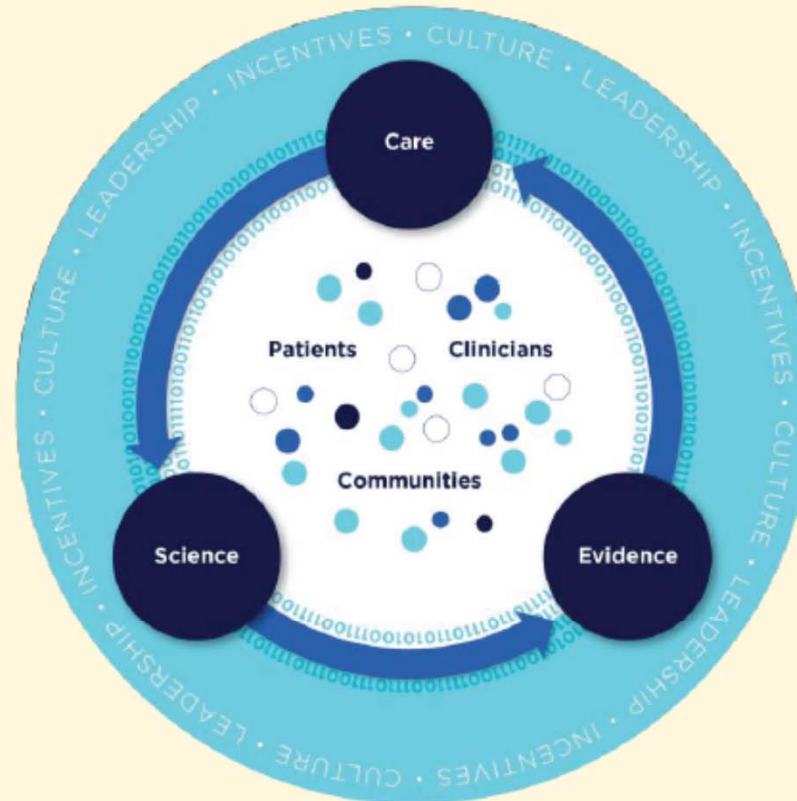
For more information visit www.iom.edu/IntegratingResearchPractice

Integrating Research and Practice: Health System Leaders Working Toward High-Value Care Workshop Summary



The Vision

Continuous Learning, Best Care, Lower Cost



INSTITUTE OF MEDICINE
OF THE NATIONAL ACADEMIES

Advising the nation / Improving health



Geisinger's Engagement Framework

Spectrum of Engagement →

Spheres of Engagement



Consultation and Disclosure



Involvement



Partnership and Shared Leadership



Leveraging the EMR and Clinical Infrastructure For Large-Scale Biobanking

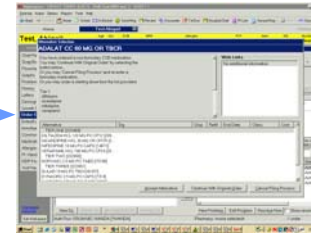
Clinic schedule and patient eligibility from EMR



Patient informed consent



Blood draw order placed in EMR



Research samples retrieved and coded



Centrally collected via Geisinger lab courier service



Blood sample collected via clinical phlebotomy



CLIA

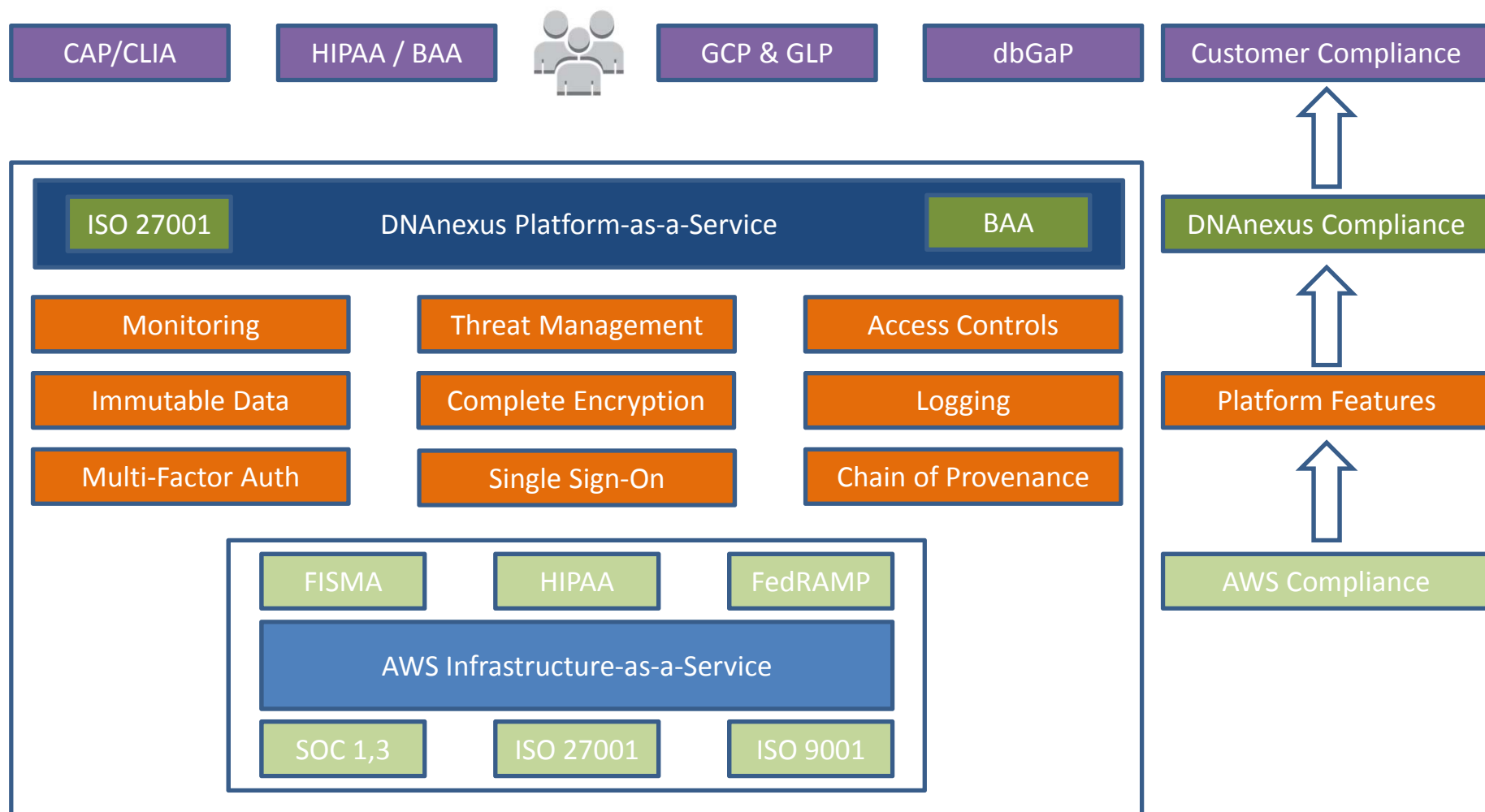
Long-term storage and tracking

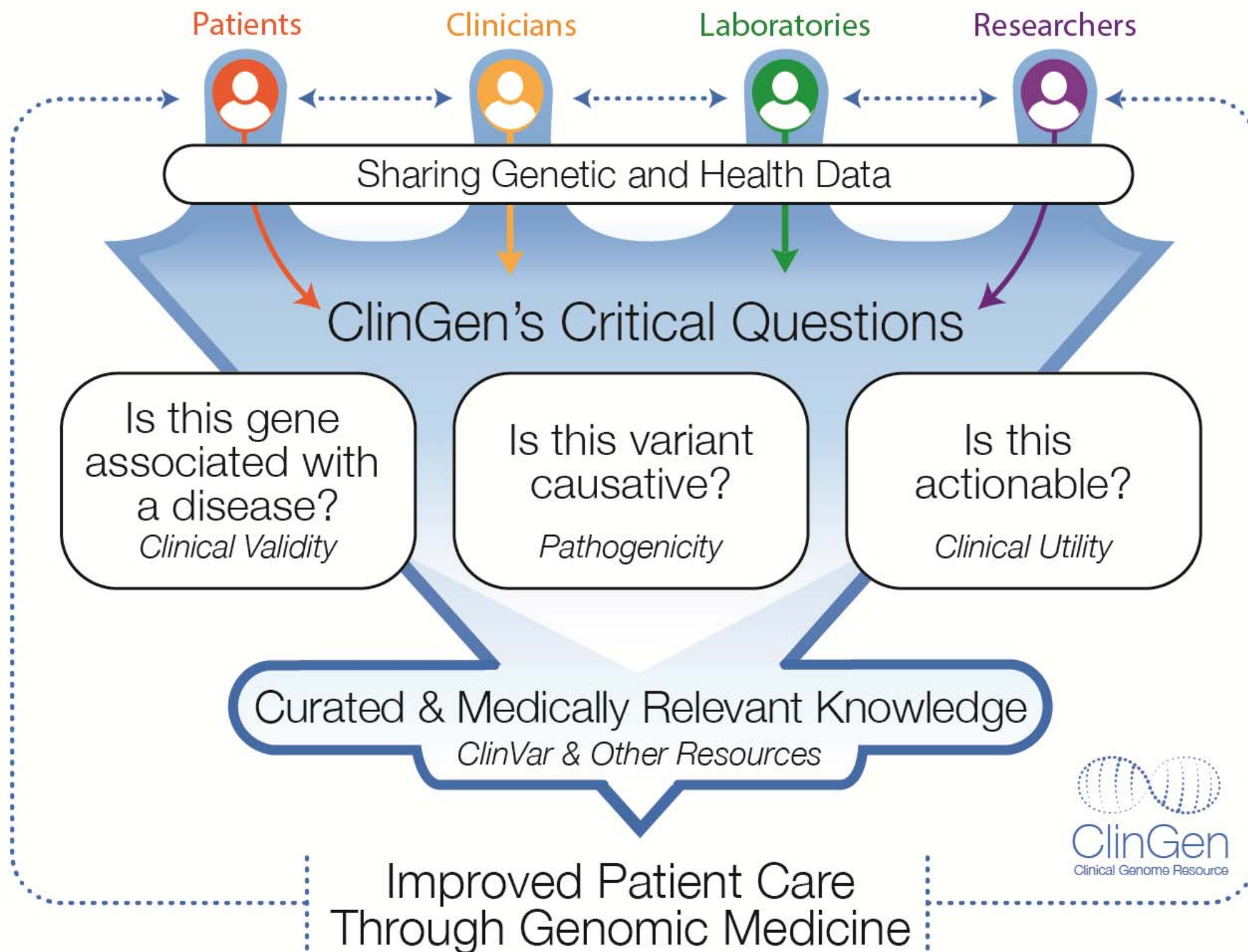


Sample analysis



DNAnexus Security Framework







GenomeConnect

The ClinGen Patient Portal

Why was GenomeConnect developed?

- *Sharing data improves patient care (increases accurate “calls” on variants)*
- *Genotype and phenotype data are often NOT available to researchers linked together*
- *Participants are often the “experts” at their medical histories*
- *Participants have a legal right to their genetic test results/reports*
- *Participants desire and benefit from connecting to each other and researchers*

HIPAA protects privacy, but FISMA protects the data

HIPAA – Protects privacy

(Health Insurance Portability and Accountability Act)

- The use and disclosure of individuals health information (protected health information)
- Sets standards for individuals' privacy rights to understand and control how their health information is used

FISMA – Secures the data

(Federal Information Security Management Act--NIST)

- Defines a comprehensive framework to protect government information systems
- Well defined process of securing, managing and monitoring government information systems

GenomeCONNECT operates as if it is subject to FISMA requirements

- PatientCrossroads (patient registry technology provider) has achieved FISMA compliance on NIH NICHD National Down Syndrome patient registry
- GenomeCONNECT utilizes the same PatientCrossroads platform and is operated in a FISMA compliant fashion in the cloud
- Should the Precision Medicine initiative consider requiring data collection systems to be FISMA compliant to secure the data?
 - Other U.S. or international standards

GEISINGER

HIPAA 2015:
Back to the Basics
What You Need To Know About
Protecting Patient Privacy
Module 1

Online: 11/1/14



HIPAA Privacy Rule: Back to the Basics

- **Unauthorized uses and disclosures** (breaches) are violations of Geisinger policy **AND** the law
- If you violate Geisinger policy and/or the law, you may be disciplined for the violation, up to and including termination of your employment



Closing Questions

- **Data quality:**
 - **Should all biospecimen collection, handling, storage be in CLIA/CAP certified laboratories? (critical for return of results)**
 - **Should all genome sequencing data be generated and analyzed in CLIA/CAP environment?**
 - **In future, will increasingly become a byproduct of routine clinical care**

Closing Questions

- **Data security/privacy:**
 - **Best practices for**
 - **technology**
 - **personnel training**
 - **monitoring/audit**
 - **Appropriate consequences for security breaches and misuse**