UPMC LIFE CHANGING MEDICINE

Privacy, Cybersecurity and the Use of Digital Health Information In Healthcare

John P. Houston, Esq.

Vice President, Privacy and Information Security & Associate Counsel

Types of Digital Health Information

UPMC has been progressive in its adoption and use of electronic heath information technologies and has amassed a significant amount of digital health information, including:

- Structured text information
- Unstructured text information
- Image and audio information
- Test results
- Genetic Information

Types of Digital Health Information

Identifiable Health Information

- Available for Treatment, Payment, Healthcare Operations (without patient consent)
- Exceptions for research

Facially De-identified Health Information

- Available for research and quality assurance purposes
- Requires execution of a Data Use Agreement

De-identified Health Information

- Available for any purpose

Digital Health Information Uses

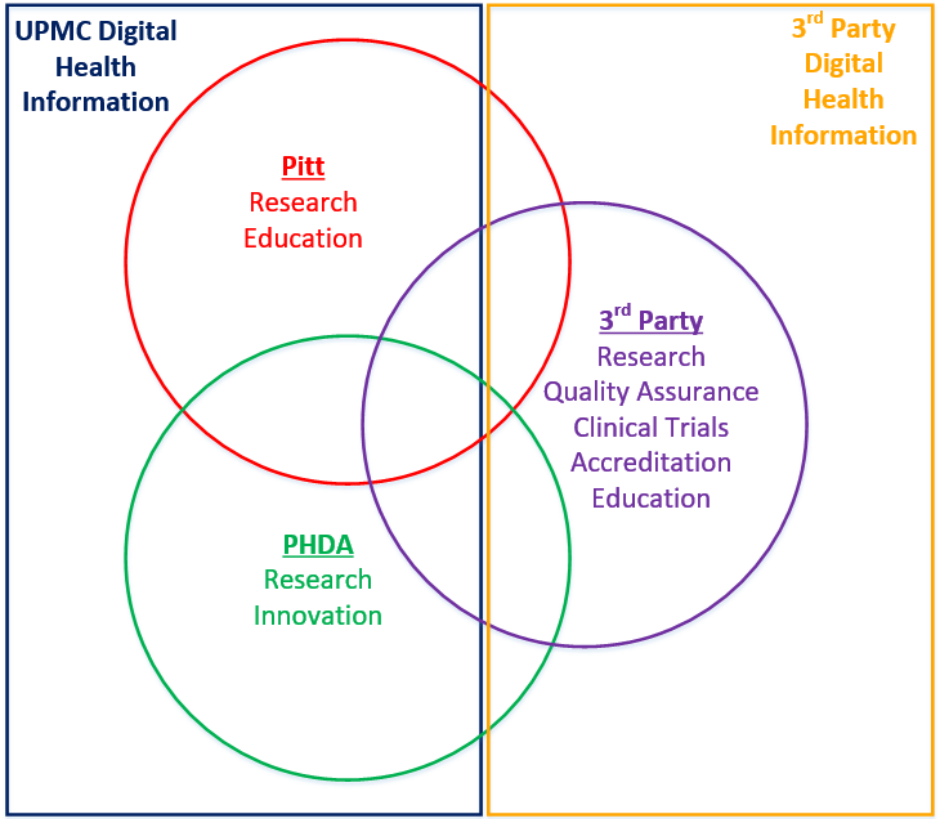
- Treatment
- Payment
- Healthcare Operations

Digital Health Information Uses

Digital health information has become increasingly used for a variety of secondary purposes, including:

- Research
- Clinical trials
- Quality assurance
- Education
- Accreditation
- Innovation

How It Fits Together



UPMC LIFE CHANGING MEDICINE

Digital Health Information

UPMC LIFE CHANGING MEDICINE

The One Constant is Change

Security is not a static discipline

- Technologies change
- Uses change
- Threats change
- Security Solutions change

Technology Changes Affecting Cyber-Security

- **The “move to the cloud” (SaaS, PaaS, IaaS, ISaaS, etc)**
- Mobile device capabilities
- Big data
- Containers
- IoT
- Data lakes

Use Changes Affecting Cyber-Security

- **Cloud delivered services**
- Mobile Device utilization
- Consumer engagement
- Big data / nano data
- The explosion of data

Threat Changes Affecting Cyber-Security

Increasing threat sophistication / complexity

- Malware / Ransomware
- DDoS Attacks
- Phishing
- Nation-state campaigns
- Advanced Persistent Threats

Security Solutions Affecting Cyber-Security

- SIEM / Analytics
- CASB
- Enhanced endpoint protection
- Identity Management
- Sandboxing
- Improved IDS / IPS tools
- Improved user authentication

The Changing Data Processing Landscape

- **Y2K**
  - 95% of all applications were run "*on-prem*"
  - 95% of all newly acquired applications run "*on-prem*"
  - Little data or "*workload*" was in the cloud
- **Today**
  - 75% of all applications run "*on-prem*"
  - Less than 20% of newly acquired applications run "*on-prem*"
  - In some form 75% of data is in the cloud
- **2022**
  - At most 25% of all applications will run "*on-prem*"
  - Less than 10% of newly acquired applications will run *"on-prem"*. Of those, most will be utility in nature
  - In some form almost 100% of data will be in the cloud

What is Driving the Move to the Cloud

- Delivery of services that have a “cloud-dependency” (such as collaboration)
- Efficiency (Maybe)
- Claims of reduced cost
- Vendor revenue

The Good…

- Improved collaboration
- Increased agility
- Reduced IT “footprint”, allowing IT to focus on “value added IT”
- Predictable operating expense
- Improved security (in some cases)

The Bad...

- Decreased data integration
- Reduced IT capability
- Additional overall expense to the organization
- Less security (in some cases)

The Ugly…

- Islands of data
- Shadow IT
- Unquantified expense to the organization
- Loss of control over security and data
- Decreased performance (when compared to “traditional IT”)
- Loss of autonomy

Questions

- How do we best manage the move to the cloud?
- How do we ensure Security?
- What happens when everything goes REALLY REALLY bad?

Issue: Security is a “Black Box"

- Often cloud service providers (CSPs) are unwilling to provide any substantive information regarding information security
- If provided, it will be limited to information related to its data center environment
- Few (if any) commitments are made regarding incident response or notification

Demand Security Transparency

- The CSP must provide information to verify that the cloud app is secure, including such things as code level reviews, pen testing, periodic patching policies, account management, etc.
- These must be done on a regular basis
- The CSP must demonstrate adoption / compliance with some type of relevant information security framework

Demand Security Transparency

- The CSP must be able to provide substantive information (and commitments) regarding how it is prepared to respond to security events
- As appropriate, the CSP should integrate into your security tools - such as Security Information and Event Management (SIEM), Identity Management (IDM) and Patient Privacy Monitoring (PPM)

Demand Security Transparency

- The CSP must be able to provide substantive information regarding security events as they happen
- The CSP must contractually agree to indemnification for breaches, as well as substantial penalties for non-performance

Issue: CSP demands rights to your data

- CSPs will often attempt to secure rights to your data
- Such rights are often broad, allowing the CSP to use (and possibly sell) your data for unrelated purposes
- Even if de-identified, data still has enormous commercial value (and could potentially disadvantage your organization in the market)

Limit the CSP's rights to your data

- Except for services that require aggregation of your data with other customers' data in order to provide the service, do not give the CSP the right to use your data
- Even where the CSP must aggregate the data to deliver the service, the use of the aggregated data should only be for the purpose of delivering the specific contracted service
- At the end of the "relationship", make sure that you get a copy of your data in a mutually agreed to electronic format (then have the vendor destroy any copies that it has)