PRIVACY AND SECURITY ISSUES IN RESEARCH: THE ONGOING STRUGGLE

MARTI ARVIN, JD, CHC-F, CCEP-F, CHPC, CHRC
CHIEF COMPLIANCE AND PRIVACY OFFICER
ERLANGER HEALTH SYSTEM

BLAZE WALESKI, JD, CIPP/US
OF COUNSEL, MOSES SINGER

1

This presentation is for general informational purposes. Nothing in this presentation should be construed as legal advice. The opinions expressed are those of the presenters and do not represent the views of their organizations.

2

2

AGENDA

- The challenges of multi-center studies, central IRBs, etc
- Big data, data retention: risk and challenges
- Secondary use of data by your organization or by others

3

3

CHALLENGES OF MULTI-CENTER TRIALS, CENTRAL IRBS, ETC.

4

4

BEFORE WE DIVE IN – BRIEF REFRESHER

- What is PHI
- What is needed for a valid authorization
- What is the Common Rule informed consent criteria

5

5

PROTECTED HEALTH INFORMATION (PHI)

HIPAA, Medical/Health Care Records

- PHI – Information identifying a patient relating to past, present or future physical or mental health or condition, or provision of healthcare, or payment thereof, and transmitted or maintained by a covered entity (HIPAA Administrative Simplification Regulations, 45 CFR § 160.103)
- May only be used and disclosed as permitted by the HIPAA Privacy Rule – Generally, a covered entity may use and disclose PHI for its own treatment, payment and health care operations activities, and related activities of another covered entity or health care provider (45 CFR § 164.502(a))
- Exceptions:
  - Per Authorization of the individual (45 CFR § 164.508)
  - Per IRB waiver or alteration of the Authorization (45 CFR § 164.512(i)(i))
  - Solely to prepare a research protocol or for similar purpose preparatory to research (45 CFR § 164.512(i)(ii))
  - Solely for research on PHI of decedents (45 CFR § 164.512(i)(iii))
  - Limited Data Set (45 CFR § 164.514(e))
    - Direct identifiers removed
    - Data Use Agreement
  - De-Identified (45 CFR § 164.514(a))

6

6

HIPAA AUTHORIZATION

Privacy Rule, 45 CFR §164.508(c)(1)

- Description of PHI
- Identification of person authorized to make use or disclosure
- Identification of person who may use the PHI
- Description of each purpose for use or disclosure (must be research study-specific, not for unspecified future research) with date or event Authorization expires
- Statement of individual's right to revoke Authorization and exceptions
- Notice of covered entity's ability or inability to condition treatment, payment, enrollment or eligibility for benefits on the Authorization, and consequences of refusal
- Potential for PHI to be re-disclosed
- Signed and dated by individual

7

7

RESEARCH DATA COMMON RULE

Informed Consent, 46 CFR § 46.116

- Applies to federally funded or regulated research of human subjects
- Investigator must obtain informed consent of subject participating in research
- Informed consent must articulate the research in sufficient detail for subject to understand reasons why or why not they might want to participate, along with specifics such as expected duration of their participation, risks, benefits, alternative procedures, extent to which records identifying them will be kept confidential, whether identifiable private information or identifiable biospecimens will be collected and if so, de-identified and used for future research

8

8

MULTI-CENTER TRIALS AND CENTRAL IRBS

- Documentation received from multi-center trials
  - Lack of ability to revise documents to fit local requirements
  - Data coming to your site as the primary data center
  - Data going to another site as the primary data center
- Other issues
  - Studies involving federal grants

9

9

DOCUMENTS RECEIVED REGARDING MULTI-CENTER TRIALS

- General approval letters
- Informed consents
- Authorizations
- Waivers of authorization
- Data use agreements

10

10

GENERAL APPROVAL LETTERS

- Letters may indicate the trial was approved but do not provide any detail for a covered entity
- There may be a statement that an authorization is needed but it is left to the researcher to ensure a valid authorization is obtained

11

11

INFORMED CONSENTS

- The ICF document may have
  - language that contradicts other documents such as the protocol, authorization, or organizational policies
  - Language inconsistent with state laws applicable to the organization
  - Language about confidentiality that are not consistent with how the study will be conducted

12

12

AUTHORIZATIONS

- A preferred centrally created authorization may not meet the needs of the organization
- If the IRB has not reviewed the authorization, researchers may not understand what is necessary to conduct the trial according to the protocol

13

13

COMBINED ICF AND AUTHORIZATIONS

- ICF includes language regarding use of data for future research but the authorization language does not
- ICF language may be inconsistent with the authorization language regarding who might see the subject's data

14

14

WAIVERS OF AUTHORIZATION

- The only documentation presented is an approval letter from a central IRB
- The data set requested does not match the approved waiver

15

15

DATA USE AGREEMENTS

- Document labeled a data use agreement (DUA) indicates
  - More than a limited data set will be shared, or
  - Does not indicate what data elements will be shared
- The researcher requests more than a limited data set
- The document labeled a DUA discusses sharing a de-identified data set

16

16

OTHER ISSUES

- Studies involving federal grants
  - Clarity around what the primary site has agreed to under the grant and what your organization is agreeing to as a sub-site
- If your organization is the primary site, ensure sub-sites understand their obligations
- Implications of an FWA for your site or for other sites in the multi-site study

17

17

BIG DATA, DATA RETENTION: RISK AND CHALLENGES

18

18

BIG DATA

- Term coined in 1998
- Large quantities of created or stored data, relative concept
- Factors:
  - Advances in storage capacity
  - Improvements in processors – Moore's Law (1965)
  - The Internet, Wi-Fi, cellular and data transfer speed
  - Other advances in information technology (IT)

19

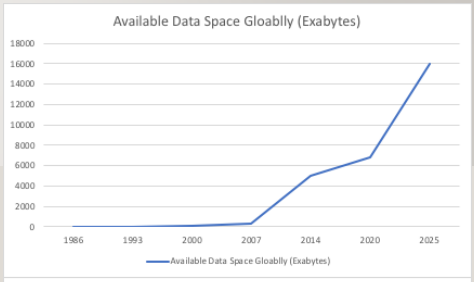
19

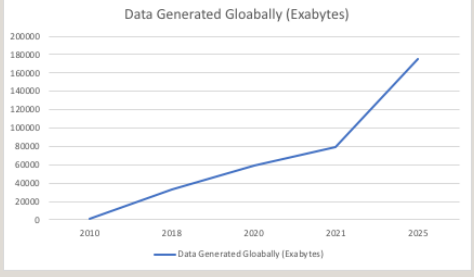
20 DATA STORAGE & GENERATION

Year	Item	Capacity	Actual Cost	Adjusted to today
1956	IBM Model 350 Disk File (size of 2 refrigerators)	5 MB	$3,200/month; $58,888	$422,847
1963	IBM first removable HDD	2.6 MB	$8,340/year	$62,575/year
1979	Seagate 5.25" HDD ST-506	5 MB	$1,588	$4,743
1980s	PCs begin to replace mainframes			
1981	IBM HDD (refrigerator size, 550 lbs.)	2.52 GB	$81,000	$204,583
1981	Apple with HDD	5 MB	$3,500	$8,840
1983	IBM PC-XT with HDD	10 MB	$7,545	$22,551
1990	Maxtor 5.25" HDD 40-100 MB available	40-100 MB		
1990	Advent of World Wide Web			
2000	Seagate Cheetah X15	18 GB	$758	$5,634
2003	Western Digital Raptor	37 GB	$119	$148
2006	Seagate Barracuda 7200.10	750 GB	$590	$671
2007	Hitachi	1 TB	$370	$489
2008	Seagate Barracuda 7200.11	1.5 TB	$160	$220
2011	Western Digital	4 TB	$300	$407
2013	Western Digital	5 TB	$300	
2018	HDDS available at 15 TB, SSD at 100 TB	15-100 TB		
2021	Seagate	20 TB	$650	
2023	Western Digital	22 TB	$449	
2026	50 TB HDD expected; 300 TB SSD	50-300 TB		
2029	100 TB HDD expected; 600 TB SSD	100-600 TB		

1 TB	=	1,000,000 MB
1 EB	=	1,000,000,000,000 MB
1 ZB	=	1,000,000,000,000,000 MB

Year	Cost per TB of storage
1956	$10,485,760,000
1980	$734,003,200
1990	$102,400,000
1995	$786,432
2000	$43,121
2010	$75
2020	$32
2023	$20





From various online sources, available upon request

20

WHY KEEP DATA? WHY NOT?

- Data has value
- Storage is relatively inexpensive and readily available (e.g., cloud offerings)
- But there are other considerations…

21

21

WHAT TO KEEP IN MIND WHEN RETAINING DATA

- Practical considerations
- Risk
- Legal compliance

22

22

PRACTICAL CONSIDERATIONS

- Data swamp versus data lake
  - Structured, access and usability
- On-site storage versus cloud
- Security
- Backup and contingency planning

23

23

RISK

- Security breach—
  - More data, more risk
  - More time, more risk (risk increases longer data is kept)
- Consequences—
  - Public relations
  - Cost
  - Time and effort
  - Legal responsibilities
  - Potential liability to individuals, contracting partners

24

24

SECURITY BREACH

Forbes.com, May 5, 2023:

"As data continues to be produced and stored in greater volumes, and as connectivity greatly expands globally on the internet, the attack surface has become more exploitable with gaps and vulnerabilities for criminal and nation state hackers. And they are taking advantage."

"In fact, the global cyber-attacks rose by 7% already in Q1 2023."

"It is estimated that 560,000 new pieces of malware are detected every day and that there are now more than 1 billion malware programs circulating."

"…so far almost 340 million people have been affected by publicly-reported data breaches or leaks in 2023…"

"While many industry sectors have been the target of cyber-attacks, including financial, education, and retail, the healthcare industry still is in the cross hairs of criminal hackers. This makes sense as many health institutions still lack the proper investment and expertise in cybersecurity because their funding goes to medical equipment and operations. Criminal hackers tend to go for the low hanging fruit."

HEALTHCARE STILL HINDERED BY CYBER ATTACKS

"According to the IBM 2022 Cost of a Data Breach report, the healthcare industry is still the costliest industry for a breach — at $10.1 million on average — for the twelfth year in a row. Fortified Health found that 78% of data breaches in 2022 were from hacking and IT incidents, an increase from 45% in 2018. Unauthorized access — the second leading cause — accounted for 38% of incidents in 2018 and now is only responsible for 16%. Other causes noted were theft, loss and improper data disposal."

"Attackers often set their sights on healthcare organizations because breaches and incidents have a high impact. Because healthcare is an essential service, organizations are more likely to pay ransoms to provide continuous care when business disruptions can have devastating consequences. Additionally, healthcare organizations possess high-value data, such as personal and financial information. Attackers can often resell records for high prices on the dark web." Hacking Caused 80% of Healthcare Data Breaches in 2022 (securityintelligence.com)

25

25

SECURITY BREACH NOTIFICATION LAWS

- HIPAA Breach Notification Rule (45 CFR §§ 164.400-414)
  - Applies to covered entities, business associates
  - Covered entity must notify individuals, media, Secretary of HHS (within 60 days)
- FTC Health Breach Notification Rule (16 CFR § 318)
  - Applies to vendors of personal health records
  - Notify individuals, media, FTC (within 60 days)
- US State Data Security Breach Notification Laws
  - Applies generally to organizations conducting business with a state
  - Notify affected individuals, sometimes state AG or agency (timing varies by state)
- Foreign Law – EU GDPR (Article 33)
  - Applies to controllers and processors of personal data of data subjects in the EU
  - Controller must notify supervisory authority within 72 hours, and data subjects in certain instances

26

26

RISK MITIGATION

- Develop and follow written policies and procedures
- Implement appropriate security protocols and controls
- Utilize 'industry standard' equipment and software
- If outsourcing (e.g., cloud)—
  - Undertake diligence of service provider
  - Have in place contracting with appropriate terms, safeguards
  - Review/audit service provider's performance
- Train staff on a regular basis
- Have a remediation plan in place before a security incident occurs

27

27

LEGAL COMPLIANCE

- Increasingly complex legal landscape—
  - US federal law, rules, regulations and guidance (e.g., HIPAA, Common Rule, consumer protection law (FTC))
  - US state law (e.g., regarding medical records, biometric data, genomics, data protection, data security, breach notification, consumer protection (state AGs))
  - Foreign law (EU GDPR, UK Data Protection Act, Canada PIPEDA, etc.)
- Consequences of non-compliance—
  - Fines and penalties
  - Civil liability
  - Public relations

28

28

HIPAA DATA RETENTION

- Administrative Simplification Regulations (45 CFR Parts 160, 162 and 164) – No records retention or deletion requirements for medical records (defer to state law)
  - But, Business Associate must return or destroy PHI at termination of BAA
- State laws governing medical records – Varying retention requirements for medical records
  - Other data protection laws may require deletion of personal information (PI)

29

29

EU LAW
GENERAL DATA PROTECTION REGULATION (GDPR)

- 'Storage Limitation' – Personal data may <u>not</u> be kept in a form that permits identification longer than necessary for the purposes for which it was collected (Article 5(1)(e))
- <u>But</u>, personal data may be stored longer if processed solely for scientific research purposes under certain conditions, so long as appropriate technical and organizational measures are implemented to safeguard the data

30

30

US STATE LAW CALIFORNIA

- California Consumer Protection Act (CCPA) (1/1/20), as amended by California Privacy Rights Act (CPRA) (1/1/23) (Cal. Civ. Code § 1798.100, *et seq.*)
- PI may be retained as reasonably necessary to achieve the purposes for which it was collected, and should then be deleted (Cal. Civ. Code § 1798.100(c))
- Also, a consumer has the right to delete PI (Cal. Civ. Code § 1798.105(a)), except for PI reasonably necessary to engage in public or peer-reviewed scientific research that conforms to applicable ethics and privacy laws, when deletion is likely to render impossible or seriously impair the ability to complete such research, if the consumer has provided informed consent (Cal. Civ. Code § 1798.105(d)(6))
- Also, CCPA/CPRA does not apply to medical records under CA law, PHI under HIPAA, PI collected in a clinical trial or other biomedical research study under the Common Rule under certain conditions (Cal. Civ. Code § 1798.145(c)(1))

31

31

SECONDARY USE OF DATA BY YOUR ORGANIZATION OR BY OTHERS

32

32

SECONDARY USE… DATA SHARING AND RE-USE

- Research data – The backbone of scientific discovery and technological innovation; prime currency of science; 'building blocks' of research
- Availability of 'Big Data' via improved storage and data transfer technologies encourages sharing and re-use
- Benefits—
  - Avoid duplication of research effort and accelerate pace
  - Save time, resources and money
  - Improve data integrity and performance
  - Enhance, validate results
  - Enhance transparency and reproducibility of the scientific enterprise
- Concerns—
  - Quality and integrity of data
  - Infrastructure of data – locating, identifying and accessing usable data
  - Legal, regulatory and ethical considerations

33

33

THE LEGALITIES OF RE-USE PERMISSION

- Does anyone assert proprietary rights in the data, and if so, do you need the right or license to use it?
- Do you need consent or authorization from individuals whose identity may be revealed by the data (PI)?

34

34

PROPRIETARY DATA

- If rights are claimed in the data, a license may be needed to use it
- The license should specify:
  - The proper field and scope of use, and 'territory' for use needed
  - The right to sublicense, if necessary
  - The duration of the license grant

35

35

LEGAL, REGULATORY AND ETHICAL CONSIDERATIONS

- What kind of data are we talking about?
- Where did it come from?
- How was it collected and for what purpose?
- For what secondary use will the data be used?

36

36

PROTECTED HEALTH INFORMATION (PHI)

HIPAA, Medical/Health Care Records

- PHI – Information identifying a patient relating to past, present or future physical or mental health or condition, or provision of healthcare, or payment thereof, and transmitted or maintained by a covered entity (HIPAA Administrative Simplification Regulations, 45 CFR § 160.103)
- May only be used and disclosed as permitted by the HIPAA Privacy Rule – Generally, a covered entity may use and disclose PHI for its own treatment, payment and health care operations activities, and related activities of another covered entity or health care provider (45 CFR § 164.502(a))
- Exceptions:
  - Per Authorization of the individual (45 CFR § 164.508)
  - Per IRB waiver or alteration of the Authorization (45 CFR § 164.512(i)(i))
  - Solely to prepare a research protocol or for similar purpose preparatory to research (45 CFR § 164.512(i)(ii))
  - Solely for research on PHI of decedents (45 CFR § 164.512(i)(iii))
  - Limited Data Set (45 CFR § 164.514(e))
    - Direct identifiers removed
    - Data Use Agreement
  - De-Identified (45 CFR § 164.514(a))

37

37

HIPAA AUTHORIZATION

Privacy Rule, 45 CFR §164.508(c)(1)

- Description of PHI
- Identification of person authorized to make use or disclosure
- Identification of person who may use the PHI
- Description of each purpose for use or disclosure (must be research study-specific, not for unspecified future research) with date or event Authorization expires
- Statement of individual's right to revoke Authorization and exceptions
- Notice of covered entity's ability or inability to condition treatment, payment, enrollment or eligibility for benefits on the Authorization, and consequences of refusal
- Potential for PHI to be re-disclosed
- Signed and dated by individual

38

38

RESEARCH DATA COMMON RULE

Informed Consent, 46 CFR § 46.116

- Applies to federally funded or regulated research of human subjects
- Investigator must obtain informed consent of subject participating in research
- Informed consent must articulate the research in sufficient detail for subject to understand reasons why or why not they might want to participate, along with specifics such as expected duration of their participation, risks, benefits, alternative procedures, extent to which records identifying them will be kept confidential, whether identifiable private information or identifiable biospecimens will be collected and if so, de-identified and used for future research

39

39

COMMON RULE

Research Data for Secondary Use

- Broad Consent (46 CFR § 116(d))
  - In lieu of study-specific informed consent, broad consent must describe:
    - Types of secondary research that may be conducted and types of institutions or researchers that may conduct the research
    - Identifiable private information or biospecimens that might be used, duration they may be stored and used, and whether they may be shared
- IRB Waiver (46 CFR § 116(f))
  - Waiver or alteration of consent permitted under certain circumstances

40

40

EU GDPR

- Applies to personal data of individuals in the EU, and the processing of personal data in the EU (Article 3)
- Comprehensive data protection law – applies to all personal data, including medical records and research data
- "Processing" of personal data – essentially everything: collecting, using, storing, disclosing, etc.
- As a general rule, the consent of a data subject is required to process personal data (Article 6(1)(a))
- Personal data may be used for secondary research that is "compatible" with the purpose for which the data was collected and consent was given (Article 6(4)), but may also be used for other purposes without consent where the processing is necessary for (see Recitals 47, 156, 157, 159):
  - "the performance of a task carried out in the public interest" (Article 6(1)(e))
  - "the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject" (Article 6(1)(f))
- A controller must "take appropriate measures" to inform data subjects of the nature of the processing activities and the rights available to them, at the time when the data is first collected or reasonably soon thereafter, and give updated notice where it intends to process data for a different purpose, including for research (Article 12(1)), except where giving such notice would be impossible or involve a disproportionate effort, or is likely to render impossible or seriously impair the achievement of the objectives of that processing (Article 14(5)(b))

41

41

US STATE LAW
CALIFORNIA – CCPA/CPRA

- Requires a business to provide notice to a CA consumer of its PI collection, use and disclosure practices (Cal. Civ. Code § 1798.100(a))
- Grants consumers rights, e.g., to correct or delete PI, and to limit the use and disclosure of sensitive PI (Cal. Civ. Code §§ 1798.105, 106, 121)
- Does not apply under certain conditions to PHI that is collected by a covered entity or business associate (Cal. Civ. Code § 1798.145(c)(1)(A)), and PI collected as part of a clinical trial or other biomedical research study subject to the Common Rule and in certain other research contexts, provided the information is not "sold" or "shared" in a manner not permitted by the CCPA, and if it is inconsistent, that participants be informed of that use and provide consent (Cal Civ. Code § 1798.145(c)(1)(C))

42

42

OTHER US STATE LAWS
VIRGINIA, COLORADO, UTAH, CONNECTICUT, IOWA, MONTANA, TENNESSEE & INDIANA

- 9 US states have enacted 'comprehensive' data protection laws loosely following GDPR (which includes California's CCPA/CPRA)
- All require notice regarding personal data collection, use and disclosure practices
- All grant consumers rights to correct (except Iowa) and to delete personal data
- All require consent to process sensitive personal data (CCPA/CPRA allows limitation)
- Each has exceptions for PHI and other medical/patient data, and regarding scientific research or "public health"; however, in varying degree and with differing conditions

43

43

US STATE LAW
WASHINGTON – MY HEALTH DATA ACT

House Bill 1155
Effective July 23, 2023

- "Information related to an individual's health conditions or attempts to obtain health care services is among the most personal and sensitive categories of data collected. Washingtonians expect that their health data is protected under laws like the health information portability and accountability act (HIPAA). However, HIPAA only covers health data collected by specific health care entities, including most health care providers. Health data collected by noncovered entities, including certain apps and websites, are not afforded the same protections. This act works to close the gap between consumer knowledge and industry practice by providing stronger privacy protections for all Washington consumers' health data."
- "With this act, the legislature intends to provide heightened protections for Washingtonian's health data by: Requiring additional disclosures and consumer consent regarding the collection, sharing, and use of such information; empowering consumers with the right to have their health data deleted; prohibiting the selling of consumer health data without valid authorization signed by the consumer; and making it unlawful to utilize a geofence around a facility that provides health care services."

44

44

Thank You!

Blaze Waleski
Of Counsel
Moses Singer
bwaleski@mosessinger.com
212-554-7843

Marti Arvin
Chief Compliance and Privacy Officer
Marti.arvin@Erlanger.org
423-778-7703

45

45