Issues related to Informed Consent:

Who has access to Research Data; Reconciling Consent and Contract Regarding Confidentiality; What Releases are required and/or allowable
## Presenters

<table>
<thead>
<tr>
<th>Presenters</th>
<th>Columbia University Medical Center</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collin R. Glidewell, JD, LLM</td>
<td>Phone: 212-305-4891</td>
</tr>
<tr>
<td>Manager of Contracts, Clinical Trials Office</td>
<td>Email: <a href="mailto:crg2148@cumc.columbia.edu">crg2148@cumc.columbia.edu</a></td>
</tr>
<tr>
<td>Karen Pagliaro-Meyer</td>
<td>Phone: 212-305-7315</td>
</tr>
<tr>
<td>Privacy Officer, HIPAA Compliance</td>
<td>Email: <a href="mailto:kpagliaro@columbia.edu">kpagliaro@columbia.edu</a></td>
</tr>
<tr>
<td>Erik Decker</td>
<td>Phone: 212-342-0268</td>
</tr>
<tr>
<td>Assistant Director, Information Security</td>
<td>Email: <a href="mailto:ed2513@cumc.columbia.edu">ed2513@cumc.columbia.edu</a></td>
</tr>
</tbody>
</table>
RECONCILING CONSENT AND CONTRACT REGARDING CONFIDENTIALITY
Reconciling Confidentiality in the Informed Consent and Contract

Informed Consent ("IC")

• What is the purpose?
• Who are the parties?
• What does the Sponsor want?
• What does the Institution want?

HIPAA Authorization

• Within the IC or in addition to the IC
Reconciling Confidentiality in the Informed Consent and Contract

**Contract**

- What is its purpose?
- Who are the parties?
- What does the Sponsor want?
- What does the Institution want?
Reconciling Confidentiality in the Informed Consent and Contract

Contract

• Confidentiality between Sponsor and Institution
  • Sponsor data
  • Institution data
  • Patient data...what should control the manner in which both parties use the Patient data?
    • Addressed in Confidentiality provision but also...
    • In Data/PHI Use provision: this is the real connection with the Informed Consent.
Reconciling Confidentiality in the Informed Consent and Contract

“Confidential Information” means this Agreement and any information that is directly or indirectly disclosed or otherwise made available under this Agreement, whether written, graphic, oral, visual, tangible or intangible, in any form or format (including machine or computer readable code). All written confidential information shall be designated as "confidential"; however, if a person in the industry would reasonably construe information disclosed hereunder as confidential, that information will be deemed confidential whether or not marked as such. For avoidance of doubt, whether or not marked confidential, any disclosures by ______ or its designees related to the Study Drug shall be treated as _____ Confidential Information for the purposes of this Agreement. Confidential Information does not include information that: (i) is now in the public domain or subsequently enters the public domain through no breach of this Agreement by the Receiving Party or its Affiliates; (ii) the Receiving Party receives from any third party that Receiving Party reasonably believed, upon reasonable due diligence, was lawfully disclosed; (iii) was in the Receiving Party’s or its Affiliates’ possession on a non-confidential basis prior to the time of disclosure by the Disclosing Party; (iv) is independently developed by or for the Receiving Party or its Affiliates by persons without access to the Confidential Information.
USE OF CONFIDENTIAL INFORMATION

The Receiving Party shall use Confidential Information solely in connection with the conduct of the Study for which it was provided or otherwise in the performance of this Agreement under which it was provided ("Permitted Purpose"). For avoidance of doubt, a Permitted Purpose includes, without limitation, publication in accordance with Article 7 (Publication) and the Parties’ determining whether or not to enter into and the negotiation of this Agreement.

PERMITTED DISCLOSURES OF CONFIDENTIAL INFORMATION

REQUIRED DISCLOSURES

RETURN OF CONFIDENTIAL INFORMATION

DURATION OF CONFIDENTIALITY
Reconciling Confidentiality in the Informed Consent and Contract

Data/PHI Use Provision:

• Sponsor will be permitted to use and disclose a Trial subject’s protected health information as permitted by the HIPAA authorization;

• Provided that neither the HIPAA authorization nor the Informed Consent will permit uses or disclosures of a subject’s protected health information that are prohibited by Privacy Laws, Laws or the conditions or limitations imposed by the IRB.

• Any modification to the form of HIPAA authorization must be approved in writing by Sponsor; notwithstanding the foregoing, as the covered entity under HIPAA,

• Institution shall have final editorial authority over the content of the HIPAA authorization.
INFORMED CONSENT
Reconciling Confidentiality in the Informed Consent and Contract

What do Sponsors want Institutions to assure them of in the Data/PHI Use provision in the Contract?

• Full access?

• Broad use?

• Place the onus on the Institution that this type of use is memorialized in the Informed Consent.
SAMPLE LANGUAGE

Will my health information be kept private?

Any information collected during this study that can identify you by name will be kept confidential. We will do everything we can to keep your data secure, however, complete confidentiality cannot be promised. Despite all of our efforts, unanticipated problems, such as a stolen computer may occur, although it is highly unlikely.

The following individuals and/or agencies will be able to look at and copy your research records:

- The investigator, study staff, {Organization Name}, {Other Organization e.g. Hospital}, and other medical professionals who may be evaluating the study

- Authorities from, {Organization Name}, {Other Organization e.g. Hospital including the Institutional Review Board ('IRB')}

- The United States Food and Drug Administration ('FDA'), the Office of Human Research Protections ('OHRP'), or other national and local health authorities

- The sponsor of this study, including persons or organizations working with or owned by the sponsor
Reconciling Confidentiality in the Informed Consent and Contract

Continued:

The study data collected, your specimens and your questionnaire responses will be assigned a code number, and separated from the patient name or any other information that could identify them. The research file that links the patient name to the code number will be kept in a secure location {inset location address} and only the investigator and study staff will have access to the file.

If the results of this research project are published or presented at a scientific or medical meeting, you will not be identified. Otherwise, all results will be kept confidential and will not be divulged (except as required by law) without permission.

You will be asked to review and sign a HIPAA Authorization form describing confidentiality.

If you refuse to provide your authorization to disclose your protected health information, you will not be able to participate in this study.

A description of this clinical trial will be available at http://www.ClinicalTrials.gov , as required by U.S. law. This Web site will not include information that can identify you. At most, the Web site will include a summary of the results. You can search this Web site at any time.
Reconciling Confidentiality in the Informed Consent and Contract

Who Controls the Informed Consent?

- The Institutional Review Board and the Sponsor
- Lack of control by Contracts Group creates an awkward situation with the Sponsor
- The Contract usually states that the Sponsor has a right of approval over IC language
- The instinct is to always make the use of data/PHI dependent upon what the approved Informed Consent permits. Why?
Reconciling Confidentiality in the Informed Consent and Contract

The IC and the Contract have conflicting statements.

What now?

• Did you make the IC the controlling document?

• If not, what next?
  • We are in breach of the contract.
  • Revise the consent, re-consent the patients.
  • What if the Study is over and patients have dispersed or not easily available?
Reconciling Confidentiality in the Informed Consent and Contract

• It is essential that information included with the sponsor protocol, the ICF and the research contract are consistent
HIPAA and Research

• HIPAA mandates that a privacy board ensure institutional compliance with HIPAA

• The role of the privacy board can be a separate function or a function that is part of the IRB

• The Privacy Rule defines the means by which individuals will be informed of uses and disclosures of their medical information for research purposes, and their rights to access information about them held by covered entities

• Where research is concerned, the Privacy Rule protects the privacy of individually identifiable health information, while at the same time ensuring that researchers continue to have access to medical information necessary to conduct vital research
<table>
<thead>
<tr>
<th>The Common Rule vs. Privacy Rule</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Common Rule is a federal policy regarding Human Subjects Protection</td>
</tr>
<tr>
<td>The main elements of the Common Rule include:</td>
</tr>
<tr>
<td>• Requirements for assuring compliance by a research institution</td>
</tr>
<tr>
<td>• Requirements for researchers’ obtaining and documenting informed consent or waiver of informed consent to participate in the research based on the risk and benefits</td>
</tr>
<tr>
<td>• Requirements for Institutional Review Board (IRB) membership, function, operations, review of research, and record keeping.</td>
</tr>
<tr>
<td>The Privacy Rule for HIPAA establishes privacy standards to protect a person’s health information</td>
</tr>
<tr>
<td>• Limits the use and disclosure of health information</td>
</tr>
<tr>
<td>• Gives patients the right to access their medical information, request amendments and restrict disclosures to the minimum intended purpose.</td>
</tr>
<tr>
<td>• Established new requirements for access to records by researchers</td>
</tr>
<tr>
<td>• Authorization generally required to use or disclose PHI except TPO</td>
</tr>
</tbody>
</table>

Institutional Review Board Annual Conference May 2014
### The Research Cycle and HIPAA Requirements

<table>
<thead>
<tr>
<th>Step</th>
<th>Approval Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generating Hypothesis</td>
<td>Review Preparatory to Research</td>
</tr>
<tr>
<td>Planning Study Design</td>
<td>Review Preparatory to Research</td>
</tr>
<tr>
<td>Identifying potential Subjects</td>
<td>Review Prep to Research/Waiver</td>
</tr>
<tr>
<td>Recruiting &amp; Enrolling Subjects</td>
<td>Waiver/Authorization</td>
</tr>
<tr>
<td>Intervention</td>
<td>Authorization</td>
</tr>
<tr>
<td>Follow-up</td>
<td>Authorization</td>
</tr>
<tr>
<td>Re-Analysis</td>
<td>Waiver/Authorization</td>
</tr>
</tbody>
</table>

**Institutional Review Board Annual Conference May 2014**
Research, Privacy & HIPAA
What Releases are required and/or allowable?

- **Consent vs. Authorization**
- **Informed Consent** is consent executed by a subject to participate in research.
- **Authorization** is permission to use the information collected for the research purpose.
- There are specific elements required within the HIPAA authorization.
- The authorization can be combined with the consent document but IRB approval is required when combined.
- Authorization to use data collected must be consistent with the consent form AND the research purpose.
- Additional Authorization required to disclose information back to treating physician or others not engaged in research.
Authorization Core Elements
(see Privacy Rule, 45 C.F.R. §164.508(c)(1))

- Description of PHI to be used or disclosed (identifying the information in a specific and meaningful manner).

- The name(s) or other specific identification of person(s) or class of persons authorized to make the requested use or disclosure.

- The name(s) or other specific identification of the person(s) or class of persons who may use the PHI or to whom the CE may make the requested disclosure.

- Description of each purpose of the requested use or disclosure. Researchers should note that this element must be research study specific, not for future unspecified research.

- Authorization expiration date or event that relates to the individual or to the purpose of the use or disclosure

- Signature of the individual and date.
Authorization Required Statements
(see Privacy Rule, 45 C.F.R. § 164.508(c)(2))

• The individual's right to revoke his/her Authorization in writing and either (1) the exceptions to the right to revoke and a description of how the individual may revoke Authorization or (2) reference to the corresponding section(s) of the covered entity's Notice of Privacy Practices.

• Notice of the covered entity's ability or inability to condition treatment, payment, enrollment, or eligibility for benefits on the Authorization, including research-related treatment, and, if applicable, consequences of refusing to sign the Authorization.

• The potential for the PHI to be re-disclosed by the recipient and no longer protected by the Privacy Rule. This statement does not require an analysis of risk for re-disclosure but may be a general statement that the Privacy Rule may no longer protect health informatio
Sample Authorization Form

FAQ’s related to research authorization

- Creation of research vs. quality databases from treatment encounters
- Is data de-identified? (not coded)
- Do I have permission to use the dataset for this research purpose?
- Is the authorization language consistent with the consent language?
- Is the authorization consistent with the research purpose?
Other use of protected health information (PHI)

• Do I have permission to use the data?
  • Where was it collected
  • Who collected the information
  • Is authorization / other IRB permission required

• Limited Data Set - Data Use Agreement
  • Can include dates, zipcode and ages
  • Requires written agreement to establish permitted use of the information
  • Must be executed if information will be disclosed outside of entity without subject authorization
  • Now covered by Breach / HITECH regulations
Omnibus
New HIPAA legislation related to Research

• Covered entities may combined “conditioned” authorizations and “unconditioned” authorization
  • For example, conditioned authorization to participate in a clinical trial may be combined with an unconditional authorization to contribute to a tissue specimen repository
  • Unconditional authorization must be opt in
    ▪ e.g. check box or second signature line
  • Authorization must clearly differentiate between conditioned and unconditioned portions
Omnibus
New HIPAA legislation related to Research

• HHS changed interpretation on authorization for future research:
  • Prior interpretation – authorization for research must be study specific
  • New Interpretation – authorization may govern future research
  • An authorization for the use of PHI for future research purposes must describe those purposes in a manner such that it would be reasonable for the individual to expect that his or her PHI could be used or disclosed for such future research.

• Decedent Information
  • No longer considered PHI 50 years after death
Business Associates & Research

- A business associate is an individual or organization that provides a service on behalf of the covered entity.
- Authorization must be obtained to disclose research subject information.
- If authorization is not obtained e.g. – waived research AND the research will use a vendor to assist in research then a business associate agreement may be appropriate.
Is a business associate contract required for a covered entity to disclose protected health information to a researcher?

Disclosures from a covered entity to a researcher for research purposes do not require a business associate contract, even in those instances where the covered entity has hired the researcher to perform research on the covered entity's own behalf. A business associate agreement is required only where a person or entity is conducting a function or activity regulated by the Administrative Simplification Rules on behalf of a covered entity, such as payment or health care operations, or providing one of the services listed in the definition of "business associate" at 45 CFR 160.103.

However, the HIPAA Privacy Rule does not prohibit a covered entity from entering into a business associate contract with a researcher if the covered entity wishes to do so. Notwithstanding the above, a covered entity is only permitted to disclose protected health information to a researcher as permitted by the Rule, that is:

- with an individual's authorization pursuant to 45 CFR 164.508,
- without an individual's authorization as permitted by 45 CFR 164.512(i),
- or as a limited data set provided that a data use agreement is in place as permitted by 45 CFR 164.514(e). [http://privacyruleandresearch.nih.gov/faq.asp#36](http://privacyruleandresearch.nih.gov/faq.asp#36)
PROTECTION OF RESEARCH DATA
Research Data Threats

Why do we care about threats to our research data?

State Sponsored Espionage

• Exploiting the “openness” of academic environments

• Compromising networks and data for competitive edge

  “...the US government claimed that the scientist provided secrets belonging to Dow AgroSciences, based in Indianapolis, Indiana, to the Hunan Normal University in Changsha, China.” (Nature, 28 July 2010)

• Traveling abroad – Foreign states will pilfer data on mobile devices. Even use hotel staff to enter hotel rooms while you are out.
Identity Theft and Fraud

• The health record contains everything needed to commit fraud.
• Not just SSN is needed!
• Name, Maiden Name, Date of Birth, Address, Nationality, Insurance numbers, credit card numbers... we collect it all.
Research Data Threats (continued)

**Regulatory or Compliance Threats**

- Required by law to monitor the data and report breaches
- Lack, or mismanagement of data protections expose researcher and University to fines and reputational embarrassment
  - Fines upwards of $1.5 million (or more, Office of Civil Rights has gone higher) (Cignet Health $4.3 million)
- Mistakes of individuals is the most common case of a breach
  - Sending PHI to inappropriate party
  - Losing unencrypted laptops
  - Policy violations
Research Data Threats (continued)

Third party requirements / Business Associates

• Two types of common research contracting:
  • Professional Services
    • Software development / Data analytics
  • IT service providers
    • Cloud / Web service providers

• Certain companies work within Healthcare space and will sign BAAs.
  • Ex: Amazon Web Services (AWS), Office 365

• Other (consumer grade) companies will not sign BAAs - not appropriate for Healthcare
  • Ex: Dropbox, Dot5Hosting, etc

• Face regulatory issues if 3rd party compromised
Data Duplication Increases Risks

Clinical systems are protected, but what about clinical research systems?

- Downstream Protection mechanisms tend to be “weaker”
- Same data, can be copied indefinitely if not careful
- Malicious individuals exploit university research systems because of this
The Various Lenses

How the Researcher See’s the Problem

• IT is not fast enough, can do it quicker on my own
• Specific and specialized needs only found in lab
• Limited amount of time and limited resources
• **Must publish!**

How the Organization See’s the Problem

• Largely de-centralized information systems.
• Immense Data Copying / Replication
  • How many copies of the same data are around the institution?
• Large amounts of complexity with very ineffective controls
• **We will have a breach!**
Data Protection Strategies of e-PHI

• Limit the scope of the data collected
  1. Remove 18 identifiers (de-identified)
  2. Limited Data Set (coded)
  3. Minimum necessary enrollments (sample size)

• Do not assume Password Protection is the best and only protection mechanism
  • Many study data security proposals read “stored on a password protected computer”. This is insufficient. With physical access:
    • Tools can hack accounts, bypassing login
    • Or just take out hard drive and attach it to another computer
Data Protection Strategies of e-PHI – 3rd Party

General Strategy: **Due Diligence and Risk Transference**

- Business Associates Agreements
- SOC 2 Type 2 reports
  - Demonstrates the company a) invests in security and b) is measured against it
- Vulnerability scanning (included in SOC 2)
- Requirement that Service Provider conducts annual Risk Analysis
- Encrypt sensitive data and do not co-mingle with other clients
- Indemnification clauses (failure to protect data indemnifies client of loss)
- Immediate notification of potential breach of e-PHI
Common Necessary and Required Controls

Processes

• Oversight of e-PHI interfaces / transfers from EHR/EMR/Billing
• IRB data security thresholds
• 3rd Party reviews by your InfoSec team

Procedures

• Access Control (who needs access)
• Authorization (what access?)
• Monitoring of e-PHI (when accessed?)
• Physical security (your locked office isn’t safe)

Technology

• Encryption
  • Hard drive (prevents loss/theft threats)
  • File & Database level (prevents malicious actor threats)
  • Transmission of data & credentials

• System updates / patching
• Limit access to Internet
• Host based firewalls
• Antivirus
Questions

FOR ADDITIONAL INFORMATION:

http://privacyruleandresearch.nih.gov

Thank you!