

Health Information Privacy & Compliance Office (HIPCO) Ancillary Review Process 2.27.18



UNIVERSITY OF MINNESOTA
Driven to DiscoverSM

HIPCO Ancillary Review Process

AGENDA

- HIPCO Role at University of Minnesota
- HIPAA Compliant Resources & Tools
- HIPCO Ancillary Review Process
- How to Ensure a Speedy HIPCO Review
- Additional Resources Available
- Questions/Comments



HIPCO Role

- Primary Responsibilities: HIPAA and health information compliance
 - UMN Policy Development & Enforcement
 - HIPAA Training
 - Investigations and Discipline
 - Coordinate with OIT and AHC-IS on security and technology matters
- Primary Objective: minimize likelihood of breaches of health information



HIPCO Role

- Recent breaches & settlements:
 - \$3.5 million - Fresenius Medical Care North America had multiple violations, including failing to encrypt PHI when it was reasonable and appropriate to do so
 - \$2.3 million – 21st Century Oncology had multiple violations, including failure to have a business associate agreement in place with a vendor and failure to have audit logs, access reports and other tracking in place with respect to PHI
 - \$2.5 million – CardioNet had multiple violations, including insufficient risk management processes
 - \$5.5 million – Memorial Health System (FL) had multiple violations, including failure to terminate logon credentials of a former employee and failure to monitor systems access and activity
 - \$3.2 million – Children's Medical Center of Dallas had multiple violations, including lack of risk management plan



HIPCO Role

- Lessons learned from settlements
 - Must have an overall security risk management plan
 - Must have current HIPAA security risk assessments
 - Must have documentation demonstrating how gaps in risk assessments are being addressed
 - Must monitor, audit and log all activity and access to PHI
 - Must have business associate agreements in place with vendors who have access to PHI



HIPAA Compliant Tools & Resources/HIPAA Center of Excellence

- AHC-IE (aka Clinical Data Repository)
- Box
- AHC-IS Servers
- AHC-IS supported PCs, laptops and other devices
- REDCap
- OnCore

- NOTE: OIT Servers are NOT HIPAA compliant!



HIPCO Ancillary Review Process

- How HIPCO Gets Involved
 - IRB Analysts assign HIPCO as an ancillary reviewer
 - When a Medical or Data/Specimen Protocol is used
 - Any time the IRB Analyst believes individual health information may be involved in the study
 - Medical & Data/Specimen Protocol templates include link to HIPCO Survey; HIPCO will provide link for other templates
- De-Identified Data
 - HIPCO reviews studies where data may be “de-identified”
 - No current process for validating de-identification of data (unless the data is provided by the AHC-IE)
- HIPCO comments are provided in ETHOS or via email to research team contact



HIPCO Ancillary Review Process

- HIPCO and IRB Reviews are separate, but:
 - HIPCO must approve the study as an ancillary reviewer before study can be finally approved by the IRB
 - IRB process can continue up to final IRB approval during HIPCO review
 - Protocol must reflect any changes to handling data resulting from HIPCO review before HIPCO can submit its ancillary review



HIPCO Ancillary Review Process

- HIPCO Review Consists of:
 - Understanding how data for the study is gathered, stored, accessed and shared
 - Directing study teams to handle data in compliance with HIPAA and UMN standards
 - Ensuring all University employed research team members have completed HIPAA16 training
 - Reviewing any HIPAA Authorization Forms
 - Reviewing any Data Use Agreements, Business Associate Agreements or similar agreements



HIPCO Ancillary Review Process

- HIPCO Survey Addresses:
 - How you will gather your research data
 - Where you will store & analyze your research data
 - How you will generate and store any links to your research data
 - Whether you will use any 3rd party devices or applications to gather, store, analyze or share data
 - How you will share your research data
 - How you will communicate with research participants



HIPCO Ancillary Review Process

- How you will gather your research data:
 - If retrieving medical records from EPIC, preferred method is use of AHC-IE
 - If collecting data directly from participants electronically, preferred method is REDCap (other tools may have to be vetted for appropriate security)
 - If receiving data from other research institutions or CMS, will need to have a data use agreement or other documentation in place



HIPCO Ancillary Review Process

- How you will gather your research data:
 - If retrieving data from a previous study or database maintained at the University, HIPCO may require
 - Documentation from the IRB approval for the previous study or database to ensure that follow up use of data has been consented to by participants, or any IRB waiver granted is broad enough to cover follow up use
 - Confirmation that the data or database is being secured in a HIPAA compliant manner



HIPCO Ancillary Review Process

- How you will gather your research data:
 - If using 3rd party vendor tools or applications
 - HIPCO will request University Information Security to review the tools/applications, and
 - a Business Associate Agreement may need to be executed (standard form BAA is in the UMN Contracts Library here:
<https://policy.umn.edu/contracts/categories/OT/240/253>)



HIPCO Ancillary Review Process

- Where you will store & analyze your research data:
 - Must use HIPAA compliant tools (AHC-IE, Box, AHC-IS Server, AHC-IS supported PCs/laptops, REDCap, Oncore)
 - If you cannot use any of the above, HIPCO will work with you to find an appropriate solution



HIPCO Ancillary Review Process

- How you will generate and store any links to your study data
 - Links cannot include research participant initials, any combination of birth dates or other dates or numbers associated with the participant
 - Links must be stored in a HIPAA compliant environment



HIPCO Ancillary Review Process

- How you will share your research data
 - Sharing research data among research team members must be done using HIPAA compliant tools (AHC-IE, Box, AHC-IS Server, REDCap, OnCore)
 - Submitting research data to sponsors can be done using the sponsor's tools



HIPCO Ancillary Review Process

- How you will communicate with research participants
 - Traditional methods: phone calls (limited voicemails), written communications, MyChart (where treatment is also involved)
 - Emails and Texts: subject to UMN Policies in Policy Library
 - <https://policy.umn.edu/operations/phi-appb>
 - <https://policy.umn.edu/operations/phi-appa>

NOTE: Any email or text to a participant includes PHI, as contact information IS PHI



How to Ensure a Speedy HIPCO Review

- **DO**

- Know where the information for your study is coming from and where it will be stored and analyzed
 - PIs – help your research team understand this so they can complete the HIPCO survey properly
- Use HIPAA compliant tools and resources for your study
 - If you cannot use the tools/resources for some reason, let us know, we cannot improve existing tools/resources if we don't know why they aren't working for you
 - We can work with you to find appropriate solutions
- Make sure the information in your protocol is consistent with information you provide to HIPCO
- Work with any vendors you will be using in advance to get Business Associate Agreements in place
- Budget for information security when submitting proposals
- Expect that the process will evolve over time!



How to Ensure a Speedy HIPCO Review

- **DO NOT**
 - Merely check the boxes for all tools listed in the HIPCO Survey, or fail to check any of the boxes
 - State that the PI says everything is OK, or that this is the way things have been done for decades
 - Use your personal laptop for storing/analyzing study data
 - Place data on thumb drives
 - Rely on having a password protected PC to store or analyze your study data
 - Withhold information because you think HIPCO doesn't need to know or wouldn't want to know
 - Hesitate to ask questions of HIPCO, your PI, or others that can provide assistance



Additional Resources Available

- For HIPAA compliant tools:
 - See information available at the [Center of Excellence for HIPAA Data](https://it.umn.edu/center-excellence-hipaa-data) (<https://it.umn.edu/center-excellence-hipaa-data>) (Box, Encrypted Email)
 - See information at the [AHC-IS web page](https://hub.ahc.umn.edu/technology-information-systems/server-operations) regarding secure, HIPAA compliant storage on AHC-IS Servers (<https://hub.ahc.umn.edu/technology-information-systems/server-operations>)
 - See information at [CTSI's website](https://www.ctsi.umn.edu/researcher-resources/clinical-data-repository) regarding the AHC-IE (clinical data repository) (<https://www.ctsi.umn.edu/researcher-resources/clinical-data-repository>)
 - See information at CTSI's website regarding [REDCap](#) and [OnCore](#)



Additional Resources Available

- For HIPAA16 Training Information:
 - See [HIPCO's website](https://www.healthprivacy.umn.edu/training)
(<https://www.healthprivacy.umn.edu/training>)
- For UMN Policies on PHI:
 - See [HIPCO's website](https://www.healthprivacy.umn.edu/guidelines-policies-procedures)
(<https://www.healthprivacy.umn.edu/guidelines-policies-procedures>)
- For Questions/Concerns:
 - Contact HIPCO at privacy@umn.edu

