# HIPAA and Academic Medical Centers Workshop

Presented by:

Michael L. Blau, Esq.
Eric B. Gordon, M.D., J.D.
McDermott, Will & Emery
mwe.com

Tina S. Sheldon
Assistant Compliance Officer
Risk Management & Audit Services
Harvard University

# Introduction

- HIPAA Challenges for AMCs
- Impact of HIPAA on Research at AMCs
- Addressing HIPAA at Harvard University

# HIPAA Challenges for AMCs

# Defining the Organization

- Hybrid entity analysis
  - Health care components don't follow departmental lines
    - Example: School of Medicine clinical education vs. pre-clinical education
  - Unsuspected health care components
    - Examples:
      - Department of Athletics
      - School of Social Work
      - On-site day care

# Defining the Organization

  - Student health center
    - Scope of FERPA exemption
    - Parents, prospective students, recent graduates, summer students...
- Affiliated entity analysis
  - Ownership or control
  - Potential issues
    - The “designated record set”
    - Accounting for disclosures
    - Implementing revocations and restrictions

# Defining the Hospital/Faculty Practice Plan Relationship

- Single covered entity/affiliated entity
- Organized health care arrangement
  - Scope of arrangement
  - Developing the joint notice
- Simultaneous consents
  - Operational issues
  - What about voluntary faculty?

# Defining the Designated Record Set

- Shadow charts
- Research charts
- Car trunk charts

# Training the Covered Workforce

- Identifying the covered workforce
- Training beyond the covered workforce (e.g., researchers)
- Method and scope of training
- Tracking results
- Enforcing the mandate
  - Physician credentialing
  - Condition of new employment/payroll

# Training the Covered Workforce

- Health profession students
- Tenured faculty

- "Secret" Workforce
  - Shared secretaries and transcriptionists
  - Volunteers
  - Students and residents

# Students and Residents

- School workforce or hospital workforce?
- Who trains?
- Resident training at practice plan sites
  - Organized healthcare arrangement?
  - Covered workforce?
  - Business associate?
  - Authorization or consent?
- Rotations to/from outside institutions

# Marketing and Fundraising in a Complex Organization

- No authorization required if
  - Fundraising is for benefit of Covered Entity only
  - Can disclose to related foundation that raises funds for Covered Entity

# Impact of HIPAA on Research at AMCs

# HIPAA and Research at AMCs

- Goal: Protect Privacy without hindering or disrupting research
- Has proper balance been struck?
- The HIPAA privacy standards will directly affect:
  - Ability of covered provider components (e.g., medical school, university health services) to obtain or use protected health information ("PHI") for research purposes (e.g., treatment-related research)

# HIPAA and Research at AMCs

- Access by AMC researchers to PHI records and databases maintained by AMC and other covered components of University
- Access by AMC researchers to PHI records and databases maintained by outside health care providers, health plans and health care clearinghouses and their business associates

- The HIPAA privacy standards will not affect:
  - Access by AMC researchers to records and databases that do not include PHI created

# HIPAA and Research at AMCs

or maintained by Covered Entities (e.g., access to governmental databases or databases from non-provider researchers/research institutions)

– Access by AMC researchers to de-identified information

# Approval for Research

- If researcher is not part of an AMC/University covered component, no additional approval is necessary to conduct research
  - Need IRB approval for human subjects research which is federally funded, federally conducted or subject to FDA jurisdiction
  - May need patient authorization/waiver of patient authorization by IRB or Privacy Board to access PHI from Covered Entities (e.g., medical center) for research purposes

# Approval for Research

- HIPAA does not protect PHI once in the hands of researchers who are not covered providers
- Four pathways to permission for Covered Entities to use or disclose PHI for research purposes:
- Pursuant to a Consent to a Covered provider for health care operations

# Approval for Research

- "Health care operations" includes protocol development; quality assurance, clinical guidelines and outcomes studies; and population-based activities relating to improving health or reducing health care costs

– Pursuant to an Authorization

- Research involving treatment of human subjects (in addition to Common Rule informed consent, where applicable)

# Approval for Research

- Authorization exceptions for protocol development and decedents

– Pursuant to a Waiver (or Alteration) of Authorization from an IRB or new Privacy Board

- Retrospective medical records or identifiable database research

– De-identification

- De-identified database research

# Consents and Authorizations: Transitional Provisions

- Pre-existing research consents and authorizations
  - General rule that pre-existing consents and authorizations are only effective for PHI created or obtained prior to compliance date
  - Special rule for research that includes treatment -- PHI created or received either before or after the compliance date may continue to be used for intended research project

# General Rule for Consents

- Covered Health Care Provider Components need Consent to use or disclose PHI for treatment, payment and healthcare operations (e.g., QA, protocol development, clinical guidelines, population-based activities)
  - Authorization required for use of psychotherapy notes
- Non-provider components (e.g., health plans) do not need Consent for these purposes
  - AMC as plan sponsor does not need Consents to use for TPO research purposes

# General Rule for Consents

- Consent must not be combined with Notice of Privacy Practices but:
  - may be part of a Research Authorization
  - may be combined with Common Rule consent if visually and organizationally separate and separately signed and dated

# Patient Authorizations

- Authorization needed when subject is available and signature may practicably be obtained
- A Covered Entity may not use or disclose PHI for any reason (other than treatment, payment, health care operations) without a valid Authorization
  - Prevents researchers from accessing PHI from Covered Entities or components for

# Patient Authorizations

most research purposes without an Authorization or Waiver

– Covered Entities can condition enrollment in research project on Authorization, other than Authorization for use of psychotherapy notes

# Obtaining Authorization

- Psychotherapy notes are notes recorded by a mental health professional documenting or analyzing the contents of conversation during a counseling session
- Psychotherapy notes do not include:
  - Medication prescription and monitoring
  - Counseling session start and stop times
  - Frequency of treatment furnished

# Obtaining Authorization

- Results of clinical tests
- Summary of diagnosis, functional status, treatment plan, symptoms, prognosis or progress

# Other HIPAA Research Issues

- Compound Authorization - Authorization may be combined with Common Rule consent for human subject research and/or Consent for TPO
  - OHRP requirements - federally funded or conducted research on human subjects
  - FDA requirements - human subject clinical trials involving drugs or devices within FDA jurisdiction

# Other HIPAA Research Issues

- Human subject research generally needs IRB approval
- Common Rule consent requirements vs. HIPAA Authorization requirements
  - Different informed consent standards
  - Different exceptions
  - May need HIPAA Authorization or Waiver in circumstances where no Common Rule consent or IRB approval required (e.g.,

# Other HIPAA Research Issues

emergency use of test article subject to FDA jurisdiction)

- Different documentation requirements -- Common Rule Waiver of documentation if consent is only record linking subject to research; or minimal risk of harm and consent is not normally required

# Comparison of and Common Rule Consent and HIPAA Authorization

## Common Rule

- Understandable language
- No exculpatory language or release of investigator, sponsor or institution
- Statement that study involves research, explanation of purposes of research, expected duration of subject's participation, description of procedures, identification of experimental procedures
- Description of reasonably foreseeable risks and discomforts to subject
- Description of benefits to subject or others reasonably expected from research
- Disclosure of appropriate alternative treatment that might be advantageous
- Statement of extent to which confidentiality will be maintained
- Explanation of whether compensation will be paid and if injury occurs, whether treatment is available and where further information may be obtained
- Explanation of whom to contact about the research, the subject's rights, and any research related injury
- Statement that participation is voluntary; refusal to participate or discontinuance carries no penalty or loss of benefits
- Statement that the treatment or procedure may involve risks to the subject which are currently unforeseeable
- Anticipated circumstances under which the subject's participation may be terminated by the investigator without regard to the subject's consent
- Any additional costs to the subject that may result from participation in the study
- The consequences of the subject's decision to withdraw from the research and procedures for orderly termination
- A statement that significant new findings developed during the course of the research which may relate to the subject's willingness to continue participation will be provided to the subject
- The approximate number of subjects involved in the study

## HIPAA Authorization

- Description of information in specific and meaningful fashion in plain language
- Name of person(s) authorized to make the requested use/disclosure
- Name of person(s) authorized to receive request
- Individual's right to revoke
- Information may be subject to redisclosure and not protected by the federal privacy regulations
- Right to inspect
- Right to refuse to authorize
- Disclose if direct or indirect remuneration to the Covered Entity will result
- Expiration date -- specific date or related event
- Signature, date
- Right to copy of Authorization

# Approval for Research

- Problems in accessing clinical databases through Authorizations
  - Specification requirement
  - Problem of unforeseen research
  - Expiration requirement - date or event
  - Problem of revocation/reliance rule
  - Problem of continuing integrity and scientific validity of database

# Comparison of Exceptions to Common Rule Consent/Authorization Requirements

**HIPAA**

- Research protocols and similar preparatory purposes
- Decedents
- FDA reports
- IRB/Privacy Board Waiver

**FDA**

- 50.23(a)-(c) Exception from the general requirements for obtaining informed consent in circumstances that are life-threatening; informed consent cannot be obtained from the subject; time is not sufficient to obtain consent from the subject's legal representative; and there is available no alternative method of approved or generally recognized therapy that provides an equal or greater likelihood of saving the life of the subject
- 50.23(d) Waiver of informed consent for military personnel -- Criteria and standards that the President is to apply in making a determination that informed consent is not feasible or is contrary to the best interests of the individual in military exigencies in accordance with the Strom Thurmond Defense Authorization Act for FY 1999

**OHRP**

- No comparable provisions

# Authorization Exceptions: Research Protocols and Decedents

- Under certain circumstances, disclosure of PHI for research is permitted without an authorization:
  - For review of PHI necessary to prepare a research protocol or for similar purposes preparatory to research
  - The disclosure is sought solely for research on decedents

# Authorization Exceptions: Research Protocols and Decedents

- Researcher must represent in writing:
  - Use or disclosure of PHI is sought solely for protocol/decedent research purposes
  - The PHI for which access is sought is necessary for research purposes
  - If protocol development, then PHI cannot be removed from premises during review
  - If decedent, documentation of death must be provided to CE upon request
- PHI related to organ donation is treated as decedent PHI

# Authorization Exceptions: Research Protocols and Decedents

- HIPAA does not address whether organs that are unsuitable for transplant can be transferred to researchers without patient Authorization

# Authorization Exception for FDA Reports

- There is an exception to the Authorization requirement for disclosure by Covered Entities that are subject to the jurisdiction of the FDA to:
  - Report adverse events to person responsible for FDA reporting
  - Enable FDA product recalls, repairs and replacements
  - Track products (as FDA-required)
  - Conduct post-marketing surveillance (as FDA-required)

# Authorization Exception: Certain Registries

- There is Authorization exception for making state and federally mandated reports
  - No Authorization exception for voluntary reports
  - No Authorization exception for privately sponsored patient registries
    - Some patient registries may qualify as business associates to whom PHI may be disclosed with patient Consent for TPO purposes (without patient Authorization)
    - Some patient registries may only receive de-identified data

# Authorizations and Consents

- Resolving conflicts between consents and authorizations
  - more restrictive governs
  - obtain new consent that clarifies
  - communicate with individual and document expressed preference

# IRB/Privacy Board Waiver

- Waivers will likely be sought for retrospective studies involving medical record reviews or database research involving PHI (i.e., patient unavailable to give authorization)
- Can obtain Waiver from any IRB or Privacy Board (no sponsorship or location requirement)
  - IRBs review federally supported or conducted research on human subjects

# IRB/Privacy Board Waiver

- IRBs review FDA human trials of FDA regulated drugs and devices
- Privacy Board may need to be formed to review: (1) research that does not involve human subjects (e.g.; database research), (2) privately sponsored research that does not involve an FDA regulated drug or device

- Duplicate or separate from IRB/Common Rule responsibilities

# IRB/Privacy Board Waiver

- Authorize access to PHI in relation to overall privacy risks vs. research project in relation to overall risks (including privacy risks)
- Different IRB exemptions for OHRP/FDA purposes mean that IRB/Privacy Board approval may be necessary for HIPAA purposes in circumstances where IRB approval would otherwise be inapplicable

# Comparison of IRB/Privacy Board Exemptions

## HIPAA

- Research protocol development
- Decedents

## FDA

46.101(b) Exemptions

- Research conducted in established or commonly accepted educational settings...
- Research involving the use of educational tests..., survey procedures, interview procedures or observation of public behavior...
- Research involving the use of educational tests (cognitive, diagnostic, aptitude achievement), survey procedures, interview procedures,.... that is not exempt if the human subjects are elected or appointed... or if these sources are publicly available...
- Research and demonstration projects which are conducted by or subject to the approval of department or agency heads, and which are designed to study... public benefit or service programs...

## OHRP

506.104 Exemptions

- Any investigation which commenced before 7/27/81, and was subject to requirements for IRB review under FDA regulations before that date, provided that the investigation remains subject to review of an IRB which meets the FDA requirements in effect before 7/21/81.
- Any investigation that commenced before 7/27/81 and was not otherwise subject to requirements for IRB review under FDA regulations before that date
- Emergency use of a test article, provided that such emergency use is reported to the IRB within 5 working days. Any subsequent use of the test article at the institution is subject to IRB review.

*Identical Exemption:*

*Taste and food quality evaluations and consumer acceptance studies, if wholesome foods without additives are consumed that contain a food ingredient at or below the level and for a use found to be safe...*

# IRB/Privacy Board Waiver

- Covered entity can accept or reject any IRB/Privacy Board decision - Waiver does not assure access to requested PHI
  - Covered entity can reasonably rely on IRB/Privacy Board
  - Joint research cooperation agreements
- To grant a Waiver (or alteration), the IRB or Privacy Board must find that Waiver would meet eight (8) specified criteria
- HIPAA Waiver criteria are different than Waiver criteria for OHRP informed consent purposes -- May meet requirements for privacy waiver but not for informed consent waiver (or vice versa)
  - No informed consent waivers for FDA clinical trials

# Comparison of Waiver of Common Rule Consent/HIPAA Authorization Requirements

## HIPAA

- 164.512(i)(2): IRB/Privacy Board must find:
  - Disclosure involves no more than minimal risk to the individual
  - Waiver or alteration will not adversely affect privacy rights and welfare of the individual
  - Research could not practicably be conducted without PHI or waiver
  - Research could not practicably be conducted without access to the PHI sought
  - Privacy risks are reasonable in relation to anticipated benefits to individuals and the importance of the knowledge that may reasonably be expected to result from the research
  - Adequate plan to protect PHI from improper use and disclosure and to destroy identifiers at the earliest opportunity consistent with the conduct of the research
  - Adequate written assurances that PHI will not be reused or disclosed

## FDA

- No comparable waiver of informed consent to clinical trials

## OHRP

IRB must find:

- 46.116(c):
  - Research conducted or subject to approval by state or local government officials to study public benefit or service programs, or changes to procedures or payment methodology, if research could not practically be carried out without waiver or alteration
- 46.116(d)
  - Research involves no more than minimal risk to subjects
  - Waiver or alteration will not adversely affect the rights and welfare of the subjects
  - Research could not practically be carried out without the waiver or alteration
  - Whenever appropriate, subjects will be provided with additional pertinent information after participation

# IRB/Privacy Board Waiver

- Issues:
  - New role for IRBs?
  - Untested standards/uncertain results What standard of "impracticality" will be applied?
    - Can't get authorizations
    - Can't be de-identified
    - Can't get determination by statistical expert
  - Destruction requirement -- unanticipated future research
  - Nonbinding decisions
  - Multi-site research (multiple IRBs/Privacy Boards)

# IRB/Privacy Board Waiver

- Waiver documentation requirements
  - Statement identifying IRB/Privacy Board
  - Date of approval
  - Statement that Waiver satisfies Waiver criteria
  - Description of PHI for which use and access has been determined necessary
  - Statement that Waiver has been approved under either normal or expedited review procedures

# IRB/Privacy Board Waiver

- Expedited review is available only if research involves no more than minimal risk to privacy
- approval by chair or designee member(s)

– Signed by chair of IRB/Privacy Board or designee(s)

– Maintain documentation for at least 6 years (current 3 year requirements for IRBs)

# IRB/Privacy Board Waiver

- IRB follows normal Common Rule requirements, including normal or expedited review procedures
- Privacy Board composition and procedures
  - Members with appropriate competency to review the effect of the research protocol on individual's privacy rights and related interests
  - At least one unaffiliated member (unaffiliated with research sponsor, Covered Entity, or their affiliates)

# IRB/Privacy Board Waiver

- No member may participate in a review of any project in which the member has a conflict of interest (employment by a covered entity that stands to gain from the research is not a disqualifying conflict)
- Approval by a majority of a quorum of members, including in the quorum at least one unaffiliated member, at a convened meeting; or approval through expedited review process by chair or designee member

# De-identified Data

- Database research involving de-identified PHI is permitted if the information does not identify an individual and there is no reasonable basis to believe the information can be used to identify an individual
- Adequate de-identification of PHI in one of two ways:
  - determination and documentation by a statistical expert that risk is very small that the information could be used to identify individual

# De-identified Data

  - Removal of 18 specified identifiers ("safe harbor")
- Identifiers include: name; birth date, admission date, discharge date, date of death (except year); ages over 89; social security numbers; e-mail addresses; medical record numbers; license plate numbers; telephone numbers; medical device identifiers/serial numbers; and for geographic region, identifiers other than state or the initial three digits of the zip code

# De-identified Data

- Any other unique, identifying number, characteristic or code
- Issues
  - Inherent identifiability of genetic information?
  - Not useful for relational databases (e.g., comparison of genetic database with clinical database)

# De-identified Data

- May not be useful for certain longitudinal studies (e.g., add new data on identifiable individuals)
- May not be useful for certain outcomes studies (e.g., inability to use date of event (other than year) may undermine study)
- May not be useful for epidemiological studies (e.g., dates needed to track disease), studies involving infants (e.g., need DOB), studies of environmental factors of disease (e.g., need zip codes)
- Paradoxically may cause researchers to seek more PHI through waiver than if de-identification standards were more reasonable
- Benchmark for determination by statistical expert
  - With genetic information may be high statistical probability of identification

# Other HIPAA Research Issues

- Identification of research subjects
- Potential lock-down of databases
- Potential delay
- Limits on retention of research data
- Business associate contracts with companies for health care diagnosis, treatment, or health care operations
  - Researchers are generally not business associates

# Other HIPAA Research Issues

  - Business associates include persons who provide data aggregation services on behalf of Covered Entity for TPO purposes (e.g., QA, population-based activities)
  - Satisfactory assurance that PHI will be appropriately safeguarded
  - Requires written contract
- Business associate contracts for reimbursement/patient assistance programs
- Accounting for research disclosures

# Minimum Information Necessary

- Minimum necessary rule compliance for Covered Entities that request, use or disclose PHI for research purposes
- Covered Entity must reasonably ensure that it does not request, use or disclose more than the minimum amount of PHI necessary
  - Reasonableness standard
  - Applies to all uses, disclosures and requests
  - Exceptions
    - providers for treatment purposes, including treatment related to research
    - Authorization
    - Required by law

# Minimum Information Necessary

- HHS for compliance purposes
- Subject individual

– No exception for PHI used for research purposes pursuant to a Consent or research that includes treatment

– Employee access policies

– Individualized determinations for non-routine uses

– Employee training

# Minimum Information Necessary

- Reasonable access controls/security measures
  - Locked file server?
  - Biometric access to server?
  - Password access
  - Employee confidentiality agreements

# Summary

- Obtain Consent for QA and other studies that involve health care operations
- Obtain authorization for other research from patients when possible
  - Require contractual affiliates to obtain Authorizations
  - May be combined with Consent/Common Rule consent
- Seek IRB/Privacy Board Waiver if patient is not available or obtaining Authorization is impractical

# Summary

- Establish a Privacy Board for privately funded research
- Consider feasibility of de-identification
  - Consider obtaining opinion of statistical expert

# AMC Research Case Studies

# Case Study 1

Dr. Ramirez has been studying the long-term effects of Marijuana use on lung function and respiratory disease in regions with varying degrees of environmental air pollution. Dr. Ramirez' study has two cohorts: one from a rural school district (clean air) and another from an inner-city school district (dirty air). The study began when participants were fifth-graders and they are now approximately 25-years-old. To remain in the study the participants must continue living in their original school districts. 72 percent of participants remain eligible. 60 percent remain in contact with the study team. The study will continue for at least another five years, funding permitting.

# Case Study 1

**Question 1: Access to which of the following sources of data for the study will be affected by HIPAA?**

- Specific health information about participants obtained by periodic interviews and lung function tests.
- Information about participants from their medical records and databases, accessed by Dr. Ramirez' team from the participants' doctors and from local hospital emergency departments, through releases originally signed by the participants' parents and then signed by the participants when they turned 18.

# Case Study 1

- Medical information about participants from their elementary and high school health clinics, obtained pursuant to releases signed by their parents.
- Death statistic information sorted by zip code and cause of death provided by the state department of vital statistics.
- Arrest records for Marijuana use/possession/sale obtained through local police blotters.
- Weekly air pollution measures of the two areas collected by the study team.

# Case Study 1

**Question 2:** **Recently Dr. Ramirez observed a correlation between the extent to which participants played organized sports in high school and their Marijuana use. Dr. Ramirez would like to analyze the data in a systematic way to further investigate this observation. The original consent forms said nothing about such an analysis.**

**What must Dr. Ramirez do from a HIPAA perspective if he wants to pursue this research topic?**

# Case Study 1

**Question 3:** **A colleague from the University of Wisconsin who has done a similar longitudinal study wants to compare her data with the data from the Ramirez study. How can Dr. Ramirez allow this under HIPAA?**

# Case Study 2

Professor McFinch wishes to study how children, whose fathers were hospitalized with a diagnosis of post-traumatic stress disorder following their military service in the Gulf War, compare to the general population for high school graduation rates. Professor McFinch, who is a clinical psychologist, has identified several potential study-participant-fathers from her private practice. She plans to contact the Veteran's Administration to locate additional individuals. Once she identifies a potential cohort, she plans to examine their V.A. hospital records to

# Case Study 2

sort potential participants by the severity and duration of their symptoms, and whether they have children in elementary or high school, as well as other factors. She then plans to contact potential participants to ask them to join the study. Once a participant joins the study, Professor McFinch will track their children until the time of their high school graduation. She also plans to gain access to their post-hospitalization treatment records.

# Case Study 2

**Question 1:** **What does Professor McFinch need to do under HIPAA to select her cohort?**

**Question 2:** **What does Professor McFinch need to do under HIPAA to conduct the study?**

# Case Study 3

For the past 25 years Professor Welty has studied surgical outcomes. She obtains data from a variety of hospitals about patients who have undergone specific surgical procedures and she follows these patients through discharge and for 2 years thereafter to determine whether they are re-admitted for post-surgical complications. Professor Welty never has direct contact with any patient and she has never obtained releases from patients. Each hospital assigns unique identifiers to the patients whose records are given to Dr. Welty. The patient's names, social security

# Case Study 3

numbers and insurance I.D. numbers are removed from the records, but all other information remains intact. Every two years, each hospital is provided its own report with a comparison of its outcomes against the other participating (but unidentified) hospitals and the hospitals use this report for quality assurance purposes. Professor Welty also publishes her results in medical journals. Her journal articles do not identify any patient, nor any participating hospitals, by name.

# Case Study 3

**Question 1:** Is the information obtained by Professor Welty de-identified?

**Question 2:** Is Professor Welty a business associate of participating hospitals?

**Question 3:** Can participating hospitals obtain the results of Professor Welty's research for quality assurance purposes? How?

**Question 4:** What must Professor Welty do to continue her research in compliance with HIPAA?

# Case Study 4

Professor Zick is a microbiologist who has discovered how to generate a protein that theoretically could dissolve the plaque that develops in the brains of Alzheimer patients, and could inhibit the development of new plaque. Professor Zick has obtained IND approval from the FDA and federal funding to test the protein in humans. He has proposed a multisite study at AMCs and nursing homes in three different regions of the country to conduct the clinical trials. The IRB at Professor Zick's university has recently approved the protocol for the clinical trial.

# Case Study 4

**Question 1:** How many different patient consents/authorizations must be obtained to conduct the clinical trials?

**Question 2:** Can a waiver of HIPAA authorization be obtained?

**Question 3:** Can all research sites rely on an IRB waiver from Professor Zick's University?

**Question 4:** What will Professor Zick need to do to assure HIPAA compliance?