



CLINICAL PATHWAYS, LLC

# HIPAA

Application in the Real World of Clinical Research:  
Updates & Current Best Practices for Successful Clinical Trials


# Disclaimer



- The content of this seminar provides information regarding the HIPAA Privacy Rule as it relates to clinical trials. The content of this presentation is not intended to provide specific legal advice. Participants should consult their legal counsel for guidance when applying the Privacy Rule to particular factual situations.



# Seminar Participant Survey

- Do you represent a:
  - Site ✓
  - Sponsor/CRO X
  - IRB 
- Do you primarily see HIPAA Authorization for Use & Disclosure of PHI:
  - Combined with ICF ✓
  - Separate from the ICF X



# Course Content

- **General: Supplements, Breaks, etc.**
- **Quick Refresher**
- **Review of the latest guidance documents and notices relating to the Privacy Rule and Clinical Research**
- **Covered Entities Compliance Update**
- **OCR Q&A relating to clinical research: Myths of Privacy Compliance**
- **Responsibilities of the study team / Application strategies for successful clinical trials**



# Quick Refresher

- The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
  - Three areas of Focus:
    - Portability of/and Access to Health Benefits
    - Preventing Fraud and Abuse in Health Care
    - **Administrative Simplification: (Save \$)**



# Quick Refresher

## Administrative Simplification

- Standardizing Electronic Financial and Administrative Data Transactions in Health Care
- Standardizing National Health Care Provider Identifiers
- Standardizing National Standard Employer Identifiers
- *Improve Privacy and Security of Health Information:  
The sections of the law that directly affect  
Clinical Research (45 CFR 160, 162, 164)*



# Quick Refresher

## Brief Chronology of the law:

- August 1996, HIPAA Passed, Public Law 104-191
- August 1999, Congress unable to agree on Privacy Rule, HHS took over
- November 1999, First Proposed HIPAA Privacy Rule, HHS
- December 2000, First Final HIPAA Privacy Regulations, HHS
- April 14, 2001, Effective Date of Privacy Regulations
  - Compliance Date: April 14, 2003
  - Except Small Health Plans may file for extension, April 14, 2004



# Quick Refresher

## Brief Chronology of the law cont.

- March 2002, Proposed Modification of HIPAA Privacy Rule
- August 2002, Final Rule as Amended from April 14, 2001; Compliance Date of Privacy Regulations still April 14, 2003
- February 2003: Final HIPAA Security Rule Regulations
- March 2003:
  - Notice of Address for Submission of Requests for Preemption Exception for State Law
  - Notice of Addresses for Submission of HIPAA Health Information Privacy Complaints



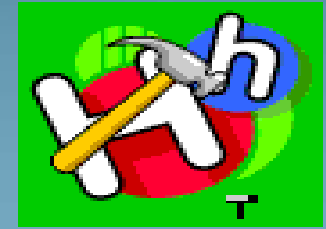
# Quick Refresher

## Brief Chronology of the law cont.

- April 2003: "Enforcement Rule" Interim Rule (45 CFR 160)
- April 2003: Security Standards Final Rule
  - *Compliance Date* April 21, 2005
  - Small health plans April 21, 2006
- April 2005: Proposed Enforcement Rule
- **February 16, 2006: Final Rule on HIPAA Enforcement Published**



# Tools & Resources



**Latest Guidance Documents and Notices Relating to the Privacy and Security Rules**

## **Sources:**

**OCR**

**NIH**

**FDA**

**State Law**

**Others**



# HIPAA Terminology

- Refer to HIPAA Terminology List
- <http://www.hipaadvisory.com/action/faqs/glossary.htm>

# OCR

## I. Website for Frequently Asked Q&A

- [http://healthprivacy.answers.hhs.gov/cgi-bin/hipaa.cfg/php/enduser/std\\_alp.php?p\\_cv=1.7%3B2.u0&%20p\\_cats=7%2C0&%20cat\\_lv11=7&cat\\_lv12=0&p\\_search\\_text](http://healthprivacy.answers.hhs.gov/cgi-bin/hipaa.cfg/php/enduser/std_alp.php?p_cv=1.7%3B2.u0&%20p_cats=7%2C0&%20cat_lv11=7&cat_lv12=0&p_search_text)
- or
- <http://www.hhs.gov/ocr/hipaa/>
  - **Click on Answers to your Frequently Asked Questions**
    - **Chose Privacy Rule Category in the drop down box.**
    - **Refer to examples Q&A Handout**

# OCR

## II. Sign up for OCR Privacy Listserv

- OCR has established a listserv to inform the public about Privacy Rule FAQs, guidance, and technical assistance materials.

- To subscribe:

<http://list.nih.gov/cgi-bin/wa?SUBED1=ocr-privacy-list&A=1>

- or you may go to <http://list.nih.gov/> and under browse, select OCR-PRIVACY-LIST.



# OCR

## III. Guidance: HOW TO FILE A HEALTH INFORMATION PRIVACY COMPLAINT WITH THE OFFICE FOR CIVIL RIGHTS

- E-mail, mail, call, fax, in person
- E-mail response to question or complaint:
  - *"Thank you for your email to the Office for Civil Rights (OCR) at the Department of Health and Human Services. This is an automated response to acknowledge receipt of your email. If your email is a complaint, it will be assigned to staff for review and appropriate action."*



# OCR

## **IV. Consumer Health Information Privacy Rights Education Booklets:**

- Your Health Information Privacy Rights
- Privacy and Your Health Information

## **V. Disclosures for Emergency Preparedness: A decision tool. (Hurricane KATRINA Bulletins I & II):**

- HIPAA PRIVACY and DISCLOSURES IN EMERGENCY SITUATIONS
- HIPAA Privacy Rule Compliance Guidance and Enforcement For Activities in Response to Hurricane Katrina & preparing for future disasters.



# DHHS / Office of the Secretary

## **VI. 45 CFR Parts 160 and 164 HIPAA Administrative Simplification Final Rule on HIPAA Enforcement; 16-FEB-2006 -Effective March 16<sup>th</sup>, 2006**

- **Adopts the Complete Regulatory Structure for implementing the Civil Money Penalty authority of the Administrative Simplification part of HIPAA.**
- **Covers the enforcement process from its beginning, which will usually be a complaint or a compliance review, through its conclusion.**



# DHHS / Office of the Secretary

## VI. HIPAA Enforcement cont.

- Principles of Achieving Compliance
  - Cooperation of CEs
  - Assistance to CEs
- Complaints:
  - Right to File a Complaint
  - Requirements for Filing
    - In writing
    - Name the person and describe the acts or omissions
    - Filed within 180 days (may be waived for good cause)
    - Secretary not required to investigate



# DHHS / Office of the Secretary

## VI. HIPAA Enforcement cont.

- Compliance Reviews:
  - Responsibility of CE
    - Provide Records and Compliance Reports (including policies regarding HIPAA)
      - During normal business hours
    - Cooperate with the investigation
    - Permit access to information (including PHI)
    - If criminal play suspected, inspection = any time



# DHHS / Office of the Secretary

## VI. HIPAA Enforcement cont.

- A complaint or compliance review may result in
  - Informal Resolution
    - If activities now satisfactory and/or implemented CAP (due diligence)
    - CE and complainant notified
  - A Finding of No Violation
    - CE and complainant notified
  - A Finding of Violation
    - CE given time to prepare defense and submit written evidence (30 days)
    - If civil money penalty imposed, CE notified
      - Notice of Proposed Determination
    - May Subpoenas witnesses and evidence



# DHHS / Office of the Secretary

## VI. HIPAA Enforcement cont.

- If a finding of a Violation is made, a civil money penalty will be sought for the violation.
  - Can be challenged by the covered entity (CE) through a formal hearing.
  - These rules apply to covered entities that violate any of the rules implementing the Administrative Simplification provisions of HIPAA



# DHHS / Office of the Secretary

## VI. HIPAA Enforcement cont.

- Civil Money Penalties
  - What if: Violation by more than one CE
    - If both at fault, each will receive penalties.
  - What if: Liability of CE due to Workforce Member actions
    - CE liable
      - Unless the agent = BA
        - The CE compliant with agreement
        - CE did not know of BA activity
        - CE would do process improvement actions



# DHHS / Office of the Secretary

## VI. HIPAA Enforcement cont.

- Civil Money Penalties
  - Amount Limitations
    - Cannot be:
      - more than \$100 for each violation or
      - in excess of \$25,000 for identical violations during a calendar year (Jan-Dec)
    - If a type of occurrence is repeated in a more general form in another situation,
      - a penalty may be imposed for a violation of only ONE of those occurrences.
    - In cases of continuing violation, a separate violation occurs each day the CE is in non-compliance.



# DHHS / Office of the Secretary

## VI. HIPAA Enforcement cont.

- Factors Considered
  - Nature and circumstances of violation
    - Results: Physical harm, hindered rights to PHI, financial harm
    - CE level of fault
    - Prior compliance hx. / repeat non-compliance
    - Compliance actions taken to date and response to previous interaction regarding inspections
    - Size and financial condition of CE



# DHHS / Office of the Secretary

## VI. HIPAA Enforcement cont.

- **Affirmative Defenses**
  - **Reasonable Cause**
    - Circumstances make it unreasonable for the CE to comply with the laws provisions
  - **Reasonable Diligence**
    - Business care and prudence expected from CE seeking to be compliant
  - **Willful Neglect**
    - Conscious, intentional failure or reckless indifference to obligations to comply



# DHHS / Office of the Secretary

## VI. HIPAA Enforcement cont.

- Cannot impose civil money penalties for:
  - Punishable under more severe requirement
  - CE did not know of the violation
  - Violation due to reasonable cause and Not willful neglect, and corrected during 30 day f/u period or during internal CAP.
- Waivers
  - In whole or part when payment would be excessive relative to the violation.
- Limitations
  - Penalties must be enacted within 6 years from the date of occurrence.



# DHHS / Office of the Secretary

## VI. HIPAA Enforcement cont.

- Notice of Proposed Determination
  - Failure to request a hearing within 90 days = imposition of the proposed penalty
  - CE may request a hearing in writing
- Notification to the public and other agencies
  - Final penalties
  - Process not organized yet



# DHHS / Office of the Secretary

## VI. HIPAA Enforcement cont.

- Due Diligence Atmosphere
- Voluntary Compliance



# NIH

- <http://www.nih.gov>
- Educational Materials
  - Authorizations
  - Clinical Research
  - Health Services Research and the HIPAA Privacy Rule
  - HIPAA Privacy Rule Booklet for Research
  - Information for Patients
  - Institutional Review Boards  
Privacy Boards
  - Research Repositories, Databases



# FDA

- Most notices from the FDA Refer to OCR (Office of Civil Rights) & CMS (Centers for Medicare & Medicaid Services)



# CMS/OCR

**Reminder: in 2002 it was established that:**

- CMS to enforce HIPAA transaction and code set standards
  - "HIPAA administrative simplification is going to streamline and standardize the electronic filing and processing of health insurance claims, save money and provide better service for providers, insurers and patients,"
  - CMS will continue to enforce the insurance portability requirements of HIPAA.

-OCR named to enforce the HIPAA privacy standards



# FDA

- **MedWatch Program: Statement on AE Reporting Post HIPAA**
- **Guidance for Industry: Institutional Review Board Review of Stand-Alone Health Insurance Portability and Accountability Act Authorizations**
- **Blood Banks & Electronic Signature Use Post HIPAA**
- **Privacy Guidance Research & IRBs**
- **Research Repositories**



# State Law

- HHS proposes that Federal laws overrule state laws that are:
  - in conflict with regulatory requirements or
  - provide less stringent privacy protections.
  - But those states that have *more* stringent privacy laws would preempt Federal law.
- State law will not be preempted unless it "prevents" compliance with HIPAA
  - State law "prevents the application" of a HIPAA provision, if the State law makes it impossible for a party to comply with HIPAA.
  - If a State law simply permits but does not require an issuer to do something that is prohibited under HIPAA, the State law would not be applicable.
    - The issuer simply could not take advantage of the more generous State law provision.
- Same approach for SOP development.



# State Law

**Specific Issue:** The previous statements regarding State laws and HIPAA have created some privacy issues. An example is the affect on telemedicine practitioners.

- Under these circumstances, telemedicine practitioners could be faced with a patchwork of state privacy standards.
  - *For example, if a specialist in state A were teleconsulting with physicians in states B, C and D,*
    - *which state privacy laws should take precedence over others?*
    - *What if they conflict?*



# State Law

- *All states have laws governing the use and disclosure of health information with a wide variety of protections.*
- *The Georgetown Privacy Project has assembled a comprehensive summary of these state laws at:*
  - [http://www.healthprivacy.org/newsletter-url2306/newsletter-url\\_list.htm?section=HPP%20Resource](http://www.healthprivacy.org/newsletter-url2306/newsletter-url_list.htm?section=HPP%20Resource)
- Search each state individually. Responsibility of the:
  - Covered Entity and/or Sponsor of Research?



# State Law

- HIPAA Preemption Charts
  - Search Each State. Example of NY
    - [http://www.health.state.ny.us/nysdoh/hipaa/hipaa\\_preemption\\_charts.htm](http://www.health.state.ny.us/nysdoh/hipaa/hipaa_preemption_charts.htm)
- Privacy Laws per State Themes:
  - Genetics
  - Vulnerable Populations
  - Others



# State Law

- Laws in every state protect the privacy of medical records to some degree.
  - Largest activity 1996-2002
- In addition, genetic-specific privacy protections exist in 28 states. (2005 statistic)



# State Law

Examples of some state laws related to genetic information and resources:

- [http://www.ornl.gov/sci/techresources/Human\\_Genome/elsi/legislat.shtml#II](http://www.ornl.gov/sci/techresources/Human_Genome/elsi/legislat.shtml#II)
- See charts of state genetics laws and information on genetics legislative activity on the **National Conference of State Legislatures Web site**.
- See the **NIH NHGRI Policy and Legislation Database** of all genetics insurance discrimination legislation.



# State Law

- Covered Entities Must know their state laws applicable to trial participant privacy.
- Sponsors & Sites that are CEs must verify that state law is included in contractual, Protocol and ICF language to protect the integrity of the data, ensure regulatory compliance & protect the rights of the study subjects. Resources:
  - Privacy Boards / IRBs
  - Legal



# Remember

## GCP and GPP:

- HIPAA Regulations do Not override The Common Rule or FDA's Human Subject's Regulations!
- HIPAA Regulations Preempts State Laws that are contrary to the Privacy Rule or offer individuals lesser protection for medical privacy or fewer right to access to health information



# Covered Entities Compliance

How has HIPAA impacted clinical researchers?



# Current Trends & Issues

## I. Increased Cost of Study Start-up

- **Additional 3 months on average**
  - Primarily due to contract language
  - Remember who is the covered entity
  - Data Use Agreements
  - Master Agreements



# Research Agreements & the Privacy Rule

- The Privacy Rule does not mandate provisions be included in research agreements between CEs and study sponsors.
  - But for CE and Sponsors to ensure the PHI of the study subjects is protected per HIPAA, inclusion of the following language in the agreements is recommended:



# Research Agreements & the Privacy Rule

- Each party's obligations to comply with all applicable laws and regulations, now including HIPAA.
  - Since most sponsors are NOT CEs, agreeing to this provision is not disadvantageous.
- The research site's (CE) responsibility to obtain the authorization of each research subject. (or waiver if applicable)
- Establish which template will be used for authorization, CEs, IRB/Privacy Board or Sponsor. (May help with missed authorizations)
- List of parties, including the sponsor, who will be permitted to receive PHI as part of the study.
- The PHI that will be permitted to be received.
- Any restrictions on the further use and disclosure of PHI by the sponsor and other parties who receive the PHI as part of the study.



# Current Trends & Issues

## I. Increased Cost of Study Start-up cont.

- Increased overhead of sites
  - Administrative Simplification
    - Privacy Officer / QA
    - Security Rule
    - National Provider Number Activities
      - Covered Entities have faced many challenges implementing HIPAA and now comes the national provider identifier rule, with a May 23, 2007, compliance date.
      - The identifier is a huge implementation issue because it involves changing information systems and business processes.
      - Several million provider identifiers need to be requested and assigned in the next 17 months.
- Increased IRB Fees (Privacy Boards)



# Current Trends & Issues

## II. Authorization: Combine or Not Combine?

- Initially separating prior to final rule
- Then combined: the amended rule allowed combining
- Now trend toward separating
  - Large institutions 50:50
  - Smaller: rely on the Sponsors approach



# Current Trends & Issues

## II. Authorization: Combine or Not Combine? Cont.

- Why separate?
  - Understanding of the participant and legal representative
  - Fear of OCR interpretation of “understandability” of the authorization language
- Why Combine?
  - Less documents to present
  - Better at wording language
- Who has the authority to decide?
  - IRB, CE, Sponsor, State Law?
- Templates
  - Added Language?



# Current Trends & Issues

## III. Release of Information

- **Institutional Policies on record review**
  - Source Document Review in the “dungeon?”
  - Appointments needing more advanced notice
  - Access to original source questionable
    - EMR vs. paper vs. shadow
- **We Must Maintain Clinical Research Best Practice when complying with HIPAA policies within the covered Entity**

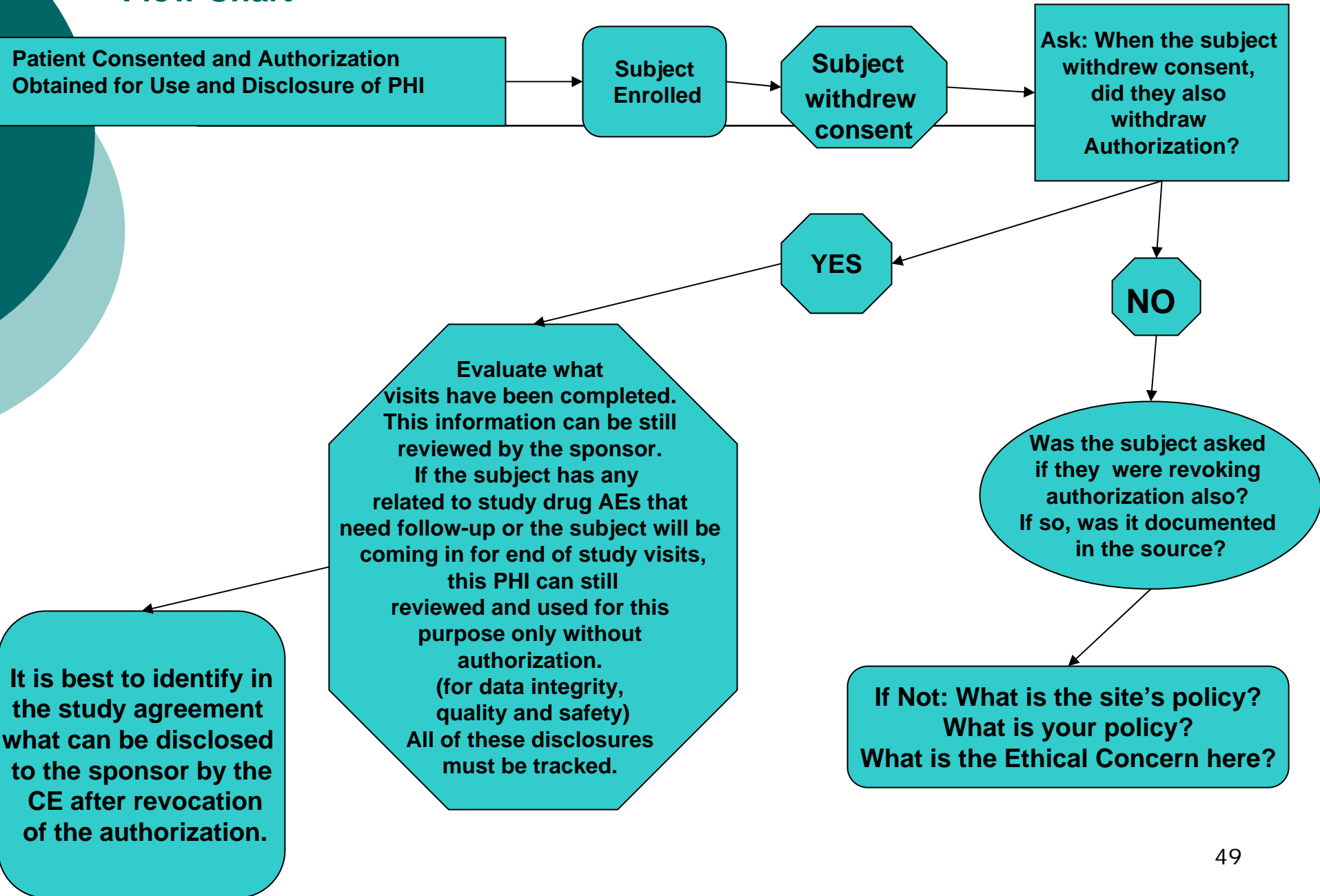


# Current Trends & Issues

## IV. Revoking of Authorization

- **Ethics: Withdraw Consent vs. Revoking Authorization**
  - **One can be verbal and one requires written request**
  - **No requirements under HIPAA that the researcher find out if a subject is revoking authorization when they are withdrawing consent.**
    - **Should this be part of the process? It is part of the consenting process.**

# Withdrawal of Consent/ Revoking of Authorization: Flow Chart





# Current Trends & Issues

## V. Compliance

- No HIPAA Privacy Inspections results directly linked to Clinical Research noted to date by the OCR.
  - We have No “Best Practice” Yet.
  - There is no such things as a HIPAA certification!
  - No mechanism in place yet to post inspection results like BIMO & OHRP
    - Final Determination of investigation
    - Complaint Driven
- **OCR stresses Due Diligence vs. Willful Neglect**
  - There have been reported cases of Research Privacy Complaints.
  - OCR Privacy Hotline 1-866-627-7748 (Little information can be obtained regarding research complaints)
  - Regional OCR Office. (For Example: NC = Atlanta 404-562-7886)



# Current Trends & Issues

## VI. The Strictest Rule . . . Rules!

- The strictest rule applies unless it contradicts Federal regulations.
- One roadblock post HIPAA is SOPs are stricter than the law.
  - Primarily found at the level of the IRB
  - Some Sponsors also



# Current Trends & Issues

## VII. HIPAA Effectiveness

- **Press February 2006 "HIPAA Ineffective", Says IT Research Group**  
(<http://www.healthprivacy.org>)
  - "With only a single conviction since its inception in 1996, HIPAA is a toothless tiger"
  - "The first problem is that HIPAA is complaint-driven, and complaint-driven enforcement doesn't work."
  - The second problem is that in the one HIPAA-related conviction that has occurred, only the individual was charged, not the organization itself.
  - If HIPAA is to be truly protective and useful, healthcare entities and their executives must be held accountable."



# HIPAA Effectiveness

## Press February 2006 Cont.

- "US agencies' commitment to enforcing HIPAA is shaky.
- A report from the Government Accountability Office (GAO) says that the FBI could not account for all of the \$379 million it was given from 2000 to 2003 in order to investigate HIPAA-related frauds. Some of the money was shifted to counter-terrorism efforts, but no one could verify that the remaining HIPAA funds were properly spent.
- One conviction that netted \$9,000 in penalties; worth an investment of over a third of a billion dollars?
- Without proper government agency oversight, it comes as little surprise that there has been only one HIPAA conviction.
- The enforcement of HIPAA is weak compared to other privacy laws such as the Fair Credit Reporting Act which earlier this month fined data broker ChoicePoint \$10 million for a security breach that resulted in the theft of 160,000 consumer records.
- The bottom line is that for HIPAA to be effective, it needs to be enforced with the same vigor that's dedicated to other laws."



# HIPAA Compliance

<http://www.hipaadvisory.com/news/>

## Unauthorized Disclosure Examples: February 9, 2006 Confidential Patient Data Sent to Wrong Companies for Months

- Case I: A small Lockport, Manitoba-based distributor of herbal remedies has for the past 15 months been mistakenly receiving faxes containing confidential information belonging to hundreds of patients with Prudential Financial Inc.'s insurance group, reports Computerworld.
  - The data exposed in the breach -- and faxed to the company by doctors and clinics across the US -- included the patients' Social Security numbers, bank details and healthcare information.



# HIPAA Compliance

[www.healthprivacy.org](http://www.healthprivacy.org)

**“Of the 19,420 grievances lodged so far, the most common allegations have been that:**

- Personal medical details were wrongly revealed
- Information was poorly protected,
- More details were disclosed than necessary,
- \*Proper authorization was not obtained,
- Patients were frustrated getting their own records.”



# HIPAA Compliance

## Most common finding in research setting is:

- No Authorization Obtained.
  - Why?
    - Most Common: The site assumed the authorization was combined. Depended on the sponsor.
- What should be done if this is found?
  - Obtain authorization ASAP.
  - Document the deficiency and what was done to address it.
  - CE to follow SOP on unauthorized disclosures (tracking)
  - Case Scenario



# HIPAA Compliance

## Documenting HIPAA authorizations in the source:

*MS. PATIENT WAS HERE TODAY FOR A SCREENING VISIT FOR THE ABC222 TRIAL. PRIOR TO INITIATION OF ANY STUDY PROCEDURES, MS. PATIENT WAS GIVEN TIME TO READ THE STUDY INFORMED CONSENT AND HIPAA AUTHORIZATION. DR. INVESTIGATOR AND MR. CRC REVIEWED THE FORMS WITH MS. PATIENT AND GAVE HER TIME TO ASK QUESTIONS. MS. PATIENT HAD QUESTIONS REGARDING EXPOSURE TO SUN LIGHT WHILE ON THE STUDY DRUG AND ACCESS TO HER STUDY RESULTS. THE KNOWN SIDE EFFECTS FOR THE PRODUCT WERE REVIEWED. MS. PATIENT WAS INFORMED THAT SHE MAY REQUEST ACCESS TO HER STUDY FILE AFTER THE STUDY DATABASE HAD BEEN SECURED BY THE SPONSOR. THE PATIENT VOLUNTARILY AGREED TO PARTICIPATE IN THE TRIAL. A SIGNED COPY OF THE INFORMED CONSENT AND HIPAA AUTHORIZATION WERE GIVEN TO THE SUBJECT.*



# HIPAA Check-up

<http://www.healthprivacy.org>

- **Bush Admin. Fails 1<sup>st</sup> and 2nd Annual HIPAA Privacy Check-Up**
- **April 14<sup>th</sup> 2004 & 2005:**
  - **Unfortunately, the impact of the Privacy Rule is dramatically weakened by rampant misunderstandings by both patients and providers and inadequate enforcement by the Bush administration.**
- **The Bush administration has been accused of failing to actively promote and enforce the Privacy Rule's language and intent**

# 1

## First Annual HIPAA Privacy Check-Up Federal Government Scoring

### 1. FAILED to educate providers and patients about responsibilities

- Misunderstandings continue to dog successful implementation of the Privacy Rule.
- A strong education effort is needed to separate myths from facts and ensure that consumers, health care providers, and insurers understand the Privacy Rule.
- \*Especially as the Bush administration is actively lobbying for the development of a national electronic medical record system (RHIOs: regional information networks and organizations)



# First Annual HIPAA Privacy Check-Up Federal Government Scoring

## RHIOs

- In 2006 new RHIOs will slowly begin to come on line in the US.
- Goal: enable clinicians to securely exchange patient medical records
- There are currently less than ten such regional information networks exchanging live data
- Predicted that approximately ten more will start operation during the course of 2006.
- Examples: CO, CT, MI, NC



# First Annual HIPAA Privacy Check-Up Federal Government Scoring

## RHIOs

- Are these systems 21 CFR 11 compliant? Will sponsor monitors / auditors have access to the original raw data?
- Consumers' privacy fears : 1 in 6 Americans withdraws from full participation in their own care because of fears that their info will be used w/out their knowledge or permission.  
\*Will this affect the recruitment for studies?



# First Annual HIPAA Privacy Check-Up Federal Government Scoring

## 2. FAILED to adequately enforce the Privacy Rule

- Relying solely on consumer complaints to enforce the Privacy Rule may not be practical.
- Despite over 11,920 consumer complaints filed, not one civil penalty has been imposed by Department of Health and Human Services. (2004)

## 3. FAILED to protect the principle of medical privacy

- U.S. Dept. of Justice (DOJ) subpoenas of medical records and many Federal policies continue to undermine the principle of medical privacy.



# First Annual HIPAA Privacy Check-Up Federal Government Scoring

## 4. FAILED to strengthen the Privacy Rule

- The Health Privacy Project's 1<sup>st</sup> *HIPAA Privacy Check-Up* called on the Bush administration to strengthen the Privacy Rule by limiting marketing to consumers and to mount a vigorous public education campaign. The administration did neither.



# Second Annual HIPAA Privacy Check-Up Federal Government Scoring

## 1. FAILED to provide adequate training and resources

- Adequate effective technical assistance to health care providers and health plans not provided.
- The administration continues to fail to educate health care consumers about their rights and health care providers about their responsibilities.

## 2. FAILED to provide adequate enforcement

- Still relying solely on consumer complaints to enforce the Privacy Rule is inadequate.
- Despite over 5,000 consumer complaints filed, not one civil penalty has been imposed by HHS.
- And, dozens of criminal complaints have been referred to DOJ, with no known penalties imposed. (April 2005)



# Second Annual HIPAA Privacy Check-Up Federal Government Scoring

- **3. FAILED to uphold the principle of medical privacy**
  - the DOJ, in its defense of the Partial-Birth Abortion Ban Act, issued subpoenas for hundreds of women's medical records.
  - In court, DOJ defended the subpoenas, arguing that "individuals no longer possess a reasonable expectation that their histories will remain completely confidential."
  - Ironically, DOJ is charged with enforcing the new Privacy Rule, which gives people exactly such an expectation of privacy.
  - Demand for the records is likely to frighten women away from certain health care services.
  - A significant percentage of people are afraid to seek care or be honest with their doctors for fear that their sensitive health information will be used against them by employers, the government, and others.



# HIPAA Homework for the Federal Government

## 1. Strengthen enforcement

- more vigilant in enforcing the Privacy Rule and must insist on full and accurate compliance.
- HHS should not rely solely on consumer-driven complaints, but should aggressively monitor and oversee compliance with the rule.

## 2. Launch an aggressive public education campaign

- public education campaign to clear up misunderstandings and illustrate that doctors, for instance, can share health information with each other without a patient's consent and that family members can be informed about a relative's condition as well as participate in health care decisions.



# Homework for the Federal Government

## 3. Limit marketing

- The Bush administration made it easier for drug companies and others to use sensitive health information to market to consumers.
- Suggested that HHS should reinstate safeguards that required drug companies and others who perform marketing on their behalf to give consumers notice and the opportunity to opt out of such marketing.

## 4. Give consumers the right to sue

- Suggest people should be able to sue when their privacy rights have been violated.
- Congress would have to amend the Privacy Rule to include a private right of action.



# Homework for the Federal Government

## 5. Conduct oversight

- Congress should hold annual oversight hearings, during which HHS will testify about complaints received, follow-up investigations, criminal referrals, public education, and enforcement.
- Congressional oversight will shed light on HHS's enforcement of the law, and provide a public record.



# HIPAA Complaints

- OCR has received more than 19,000 complaints since 2003. Despite HIPAA's establishment of civil penalties for violations of the privacy law, OCR has yet to impose a single civil penalty.
- For a partial list of reported privacy violations, see HPP's "Medical Privacy Stories."

[http://www.healthprivacy.org/info-url\\_nocat2303/info-url\\_nocat\\_show.htm?doc\\_id=367663](http://www.healthprivacy.org/info-url_nocat2303/info-url_nocat_show.htm?doc_id=367663)



# HIPAA Prosecutions

**2 Federal criminal prosecutions under HIPAA since it took effect in April, 2003:**

#1: A Washington state man employed at a Seattle cancer treatment center was convicted in 2004 after admitting he used protected medical records to obtain a patient's name, date of birth and Social Security number to obtain four credit cards in the patient's name.

#2: March 28, 2006: Medical office staffer admits selling unique health identifiers; a Texas woman was convicted in federal court on March 6 after pleading guilty to felony charges of wrongful use of unique health identifiers. She was arrested after agreeing to sell individually-identifiable medical information about FBI agents to an informant she believed to be working for a drug trafficker.



# HIPAA Prosecutions

## What may be #3: May 2006

The names, birth dates, Social Security numbers, and, in some cases, disability ratings of as many as 26.5 million veterans were stolen recently from the home of a Department of Veterans Affairs employee on May 3 in suburban Maryland. The employee was not authorized to remove the sensitive information. This theft represents the biggest unauthorized disclosure of Social Security data ever.

## What about Research Specific?

- Queries to OCR, FDA, [www.healthprivacy.org](http://www.healthprivacy.org) to date



# HIPAA Compliance

The reporting system for HIPAA inspection results is still not organized yet. Even though we do not have specific reports for research, we need to be sure we have compliance review in the CE.

- What have you in place to identify issues?
- Do your employees ever remove data from the workplace?
- Is there any practices at work that potentially jeopardize the security of identifiable information?
- How is the patient educated regarding the security of their PHI, even when it is shared outside the CE (research)



# Privacy Rule's Security

- Distinction Between the Security and Privacy Rule?
  - Inextricably Linked
  - Compliance April 20<sup>th</sup>, 2005
  - Security of the electronic form of PHI
    - Standards
    - Implementation Specifications
  - Privacy Rule looks at PHI in any form.
- 21 CFR part 11 preparedness
  - Sites, vendors, sponsors, CRO, etc.
  - Issues with HER or EMR



# Myths of HIPAA

Healthcare-Provider-letter myths: [www.healthprivacy.org](http://www.healthprivacy.org)

Myth #1: **One Doctor's office cannot send medical records of a patient to another doctor's office without patient's consent.**

Myth #2: The HIPAA Privacy Regs prohibits or discourages doctor/patient emails.

Myth #3: A patient cannot be listed in a hospital's directory w/out the pts consent and the hospital is probited from sharing a pts directory info with the public.

Myth #4: Members of the clergy can no longer find out whether members of their congregation or religious affiliation are hospitalized unless they know the person by name.

Myth #5: **A hospital is prohibited from sharing info with the pts family w/out the pts express consent.**



# Myths of HIPAA

Healthcare-Provider-letter myths: [www.healthprivacy.org](http://www.healthprivacy.org)

**Myth #6: A pts family member can no longer pick up prescriptions for the pt.**

**Myth #7: The privacy regulation mandates all sorts of new disclosures of pt info. (oversight of investigation, to the individual upon request and for TPO)**

**Myth #8: The HIPAA Privacy regulations impose so many administrative requirements on CEs that the costs of implementation are prohibitive.**

(2002 report from WHO 10 yrs = \$18 billion / estimate of savings = \$29.9 linked mainly to the transaction standards. No account for negative impact on research and other fields.)



# Myths of HIPAA

Healthcare-Provider-letter myths: [www.healthprivacy.org](http://www.healthprivacy.org)

Myth #9: Pts will sue health care providers for not complying with the HIPAA Privacy Regs.

Myth #10: Pts medical records can no longer be used for marketing.

Myth #11: If a pt refuses to sign an acknowledgement stating that they received notice of privacy practices, the provider can, or must refuse to provide services.

Myth #12: The HIPAA Privacy Rule imposes many new restrictions on hospitals' funding efforts so that fundraising becomes almost impossible.

Myth #13: The press can no longer access vital public info from hospitals about accident or crime victims.



# More HIPAA Myths from the OCR

## OCR Q&A relating to Clinical Research: Myths of Privacy Compliance



# Question I

- Does the Privacy Rule permit a covered entity to use or disclose protected health information pursuant to an Authorization form that was prepared by a third party?



# Answer

- Yes.
- A covered entity is permitted to use or disclose protected health information pursuant to any Authorization that meets the Privacy Rule's requirements at 45 CFR 164.508.
- The Privacy Rule requires that an Authorization contain certain core elements and statements,
  - \*but does not specify who may draft an Authorization (i.e., it could be drafted by any entity)
  - \*or dictate any particular format for an Authorization.



# And

- Thus, a covered entity may disclose protected health information as specified in a valid Authorization that has been created by another covered entity or a third party, such as an insurance company or researcher.



## Question II

- Must a covered health care provider obtain an individual's authorization to use or disclose protected health information to an interpreter?



# Answer

- No
- When an interpreter is used to communicate with an individual, the individual's authorization is not required.
- Covered entities may use and disclose protected health information for treatment, payment and health care operations without an individual's authorization, 45 CFR 164.506(c).
- A covered health care provider might use interpreter services to communicate with patients who speak a language other than English or who are deaf or hard of hearing, and provision of interpreter services usually will be a health care operations function of the covered entity as defined at 45 CFR 164.501.



# And

- The interpreter may be internal or external to the company:
  - When the interpreter is a member of the covered entity's workforce (i.e., a bilingual employee, a contract interpreter on staff, or a volunteer) as defined at 45 CFR 160.103;
  - When a covered entity engages the services of a person or entity, who is not a workforce member, to perform interpreter services on its behalf, as a business associate, as defined at 45 CFR 160.103.
    - A covered entity may disclose protected health information as necessary for the business associate to provide interpreter services on the covered entity's behalf.
      - Business Associate Agreement



# Question III

- Can a physician's office FAX patient medical information to another physician's office?



# Answer

- Yes
- The HIPAA Privacy Rule permits physicians to disclose protected health information to another health care provider for treatment purposes. Research is considered treatment.
- This can be done by fax or by other means like phone.
- Covered entities must have in place reasonable and appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information that is disclosed using a fax machine.



# And

- Examples of measures that could be reasonable and appropriate in such a situation include:
  - the sender confirming that the fax number to be used is in fact the correct one for the other physician's office, and
  - placing the fax machine in a secure location to prevent unauthorized access to the information. See 45 CFR164.530(c).
  - Document these efforts!



# Question IV

- Can the Review Preparatory to Research (RPR) provision of the HIPAA Privacy Rule at 45 CFR 164.512(i)(1)(ii) be used to recruit individuals into a research study?



# Answer

- Yes
- This provision permits covered entities to use or disclose protected health information for purposes preparatory to research, such as to aid study recruitment.
- However, the provision at 45 CFR 164.512(i)(1)(ii) does not permit the researcher to remove protected health information from the covered entity's site.



# And

- A researcher who is an employee or a member of the covered entity's workforce could use protected health information to contact prospective research subjects.
  - The preparatory research provision would allow such a researcher to identify prospective research participants for purposes of seeking their authorization to use or disclose protected health information for a research study.
- A researcher who is Not a part of the covered entity may not use the preparatory research provision to contact prospective research subjects unless partial waiver is approved by the IRB/Privacy Board.
  - The outside reviewer can give the information to the CE to contact the patient for the study.



# Exception

- Use of RPR for recruitment screening is challenging for the Common Rule (45CFR46)
  - Must do waiver of consent plus the RPR.
  - Therefore, tend to do Waiver of Authorization instead of RPR.
  - RPR reserved more for grant proposals or study feasibility analyses.



# Question V

- Does the HIPAA Privacy Rule permit the creation of a database for research purposes through an Institutional Review Board (IRB) or Privacy Board waiver of individual authorization?




# Answer

- Yes
- A covered entity may use or disclose protected health information without individuals' authorizations for the creation of a research database,
  - provided the covered entity obtains documentation that an IRB or Privacy Board has determined that the specified waiver criteria were satisfied.
- Protected health information maintained by a covered entity in such a research database could be used or disclosed for future research studies in which
  - individual authorization has been obtained or
  - where the Rule would permit research without an authorization, such as pursuant to an IRB/Privacy Board waiver.



# Question VI

- Does the HIPAA Privacy Rule require a covered entity to create an Institutional Review Board (IRB) or Privacy Board before using or disclosing protected health information for research?



# Quick Note About Privacy Boards


- A board that may be created by the CE to review the researchers requests for:
  - Waiver or Alterations of the requirements for individual authorization per the Privacy Rule.
  - May use an IRB to perform these activities.
  - Can be external to the CE if proven reliable.
- Not required to have a minimum number of members, but must have varying backgrounds and appropriate professional competency.
- Must include at least one unaffiliated member.
- Members may not participate if they have a conflict of interest with the research.



# Answer

- So the answer is . . . No
- The IRB or Privacy Board could be created by the covered entity or the recipient researcher, or
- It could be an independent board.

# Question VII

- 
- Subject Revoking Authorization
    - Scenario: During a site visit a research nurse informs the study monitor that there has been follow-up information obtained for a subject that is no longer participating in the trial and has also revoked authorization prior to this follow-up.
      - Can the CRC disclose the details of the event to the CRA?



# Answer

- Yes.
- 45 CFR 164.508 & 164.512(b)
- “HIPAA allows covered entities to use and disclose information without patient authorization or waiver for purposes related to the
  - quality, safety, or effectiveness of FDA-regulated products.
    - Examples include: adverse events, device tracking, recall, post marketing surveillance.”
      - End of study visits, reasons for termination, regulatory inspections
  - Disclosures must be tracked.

# Question VIII

- 
- What does the HIPAA Privacy Rule say about a research participant's right of access to research records or results?



# Answer

- With few exceptions, the Privacy Rule gives patients the right to inspect and obtain a copy of health information about themselves that is maintained by a covered entity or its business associate in a “designated record set.”
- A designated record set is basically a group of records which a covered entity uses to make decisions about individuals.



# And

## Permitted Exception

- clinical trial data:
  - The Privacy Rule permits the individual's access rights in these cases to be suspended while the clinical trial is in progress,
    - provided the research participant agreed to this denial of access when consenting to participate in the clinical trial.
  - In addition, the health care provider/researcher must inform the research participant that the right to access protected health information will be reinstated at the conclusion of the clinical trial.



# Question IX

- Does the HIPAA Privacy Rule prohibit researchers from conditioning participation in a clinical trial on an authorization to use/disclose existing protected health information?



# Answer

- No.
- The Privacy Rule does not address conditions for enrollment in a research study.
- Therefore, the Privacy Rule in no way prohibits researchers from conditioning enrollment in a research study on the execution of an authorization for the use of pre-existing health information.
- Current Practice: Yes, refusal of authorization = ineligibility to participate. The data could not be reviewed or collected.



# Question X

- Does HIPAA allow the authorization for disclosure of PHI for a clinical trial be combined with an authorization that would permit PHI collected during a trial to be placed in an archive or database for future research uses.



# Answer

- No.
- Since the participation in the clinical trial depend upon the subject signing an authorization specific to the trial, combining the two different authorizations together conditions their participation in the trial on future use of the information and the patient should be able to say NO to this separate disclosure and still be able to participate in the trial.
- This would be considered coercive.
- Remember the authorization must be specific to the protocol, not a blanket institutional authorization.



# Responsibilities of the Study Team: Site (CE)

- CE HIPAA Policy Creation and Maintenance Mandatory
- Minimal Requirement of Policy:
  - Approved by Senior Management
  - Appoint Security and Privacy Official
  - Required Training
    - How Much?
    - How Often?
  - Covers All Requirements of Law
    - Can be more impacting
    - Cannot contradict
- This includes authorized and unauthorized disclosures



# Responsibilities of the Study Team: Site (CE) cont.

- Must store 6 years from creation or last in effect
  - All documents, templates, authorizations, agreements
  - Annual Compliance Report Required
    - Content? Not specified.
    - Send when and where? Not Specified.
- Staff must be trained per regulations regarding HIPAA
- Apply GCP and GPP to study management
  - Risk analysis of depending on study sponsors for authorizations content
  - Know policies of HIPAA privacy board or IRB if applicable
- List methods to stay current with regulations
- Evaluate site privacy and security practices\*



# Responsibilities of the Study Team: Sponsor

- Assess compliance of current or potential sites  
<http://www.hhs.gov/dab/search.html>
- Identify when provisions of assurance of protection of privacy of PHI is needed. (Research Agreement)
- Recognize study practices that may create conflict in site compliance
- Defend the need for previously collected data after subject revocation of authorization
- Verify sites process for obtaining authorizations



# Responsibilities of the Study Team

## Practices that Cause Conflict in Compliance

- Pre-screening Logs (unauthorized disclosures)
- Sponsor SOPs that require sites to ? if GPP
- Adopt new practices during the different stages of a clinical trail
- Evaluate the need to revise current study templates
- Develop methods to provide essential documentation of compliance



# Responsibilities of the Study Team

## Sites & Sponsors

- Development & Approval of research policies & procedures to support HIPAA:
  - Start at Evaluation / Site Selection Visits
    - Preliminary Questions to Answer
  - Master Agreements
  - Initiation Visit



# Responsibilities of the Study Team

## Site Visit Report Revisions:

- **Evaluation Visits**
  - **Addition of Site HIPAA Compliance Questions**
    - **Include Action Plans for Compliance and Timelines for Assurance Requirements**
    - **Example Questions**



# Responsibilities of the Study Team

## Initiation Visits and/or Investigator Meeting:

- Addition of Site HIPAA Compliance Questions:
- Include Action Plans for Compliance: Risk of Unresolved Action Items
- Document Statement of Assurance of Protection of PHI
- Site's Requirements



# Responsibilities of the Study Team

## Interim Monitoring Visits:

- List How, When, and by Whom Authorization was obtained
- Monitor for an Revoking of Authorization and Changes in Privacy Practices
- Careful to Add Action Items for GPP and Follow through



# Responsibilities of the Study Team

## Close-out Visit:

- Reassurance
- Action Item Resolution



# Responsibilities of the Study Team

## Follow-Up Letters

- Document Authorizations
- Document GPP



CLINICAL PATHWAYS, LLC

## Summary:

Let's work together to uphold the Privacy of Clinical Research Participant Data; then ultimately we will increase the confidence of the general public in Clinical Trials.



CLINICAL PATHWAYS, LLC

# Q & A

# THANK YOU!

[samsather@clinicalpathwaysresearch.com](mailto:samsather@clinicalpathwaysresearch.com)