

# **Conducting Clinical Trials Under HIPAA - Implications For Sponsors**

---

## **Pharmaceutical Regulatory and Compliance Congress and Best Practices Forum**

**Philadelphia, November 13-15, 2002**

**Carol A. Pratt, Ph.D., JD**

**Davis Wright Tremaine LLP**

**Portland, OR**

Seattle, San Francisco, Los Angeles, NY,  
Wash.. DC, Anchorage, Honolulu

**(503) 778-5279**

**[carolpratt@dwt.com](mailto:carolpratt@dwt.com)**

Copyright 2002 Carol A. Pratt

# HIPAA's Privacy Rule For Research

---

- A covered entity may not *use or disclose*
- Protected health information (PHI)
- Without written *authorization* – **UNLESS**
  - Qualifies for a waiver of authorization
  - An exception applies
  - Disclosure to a business associate
  - Permitted disclosures

# Minimum Necessary Rule

---

- CE must make reasonable efforts
- When using, *disclosing* or requesting PHI from another CE
- To limit PHI to the minimum necessary to accomplish the intended purpose
  - CE may not use an entire medical record unless it can justify that it is the minimum necessary
- Does *not* apply to:
  - Disclosures to the individual
  - Use/disclosure pursuant to an authorization

# HIPAA's General Research Rule

---

**Research + CE + PHI = HIPAA  
Authorization**

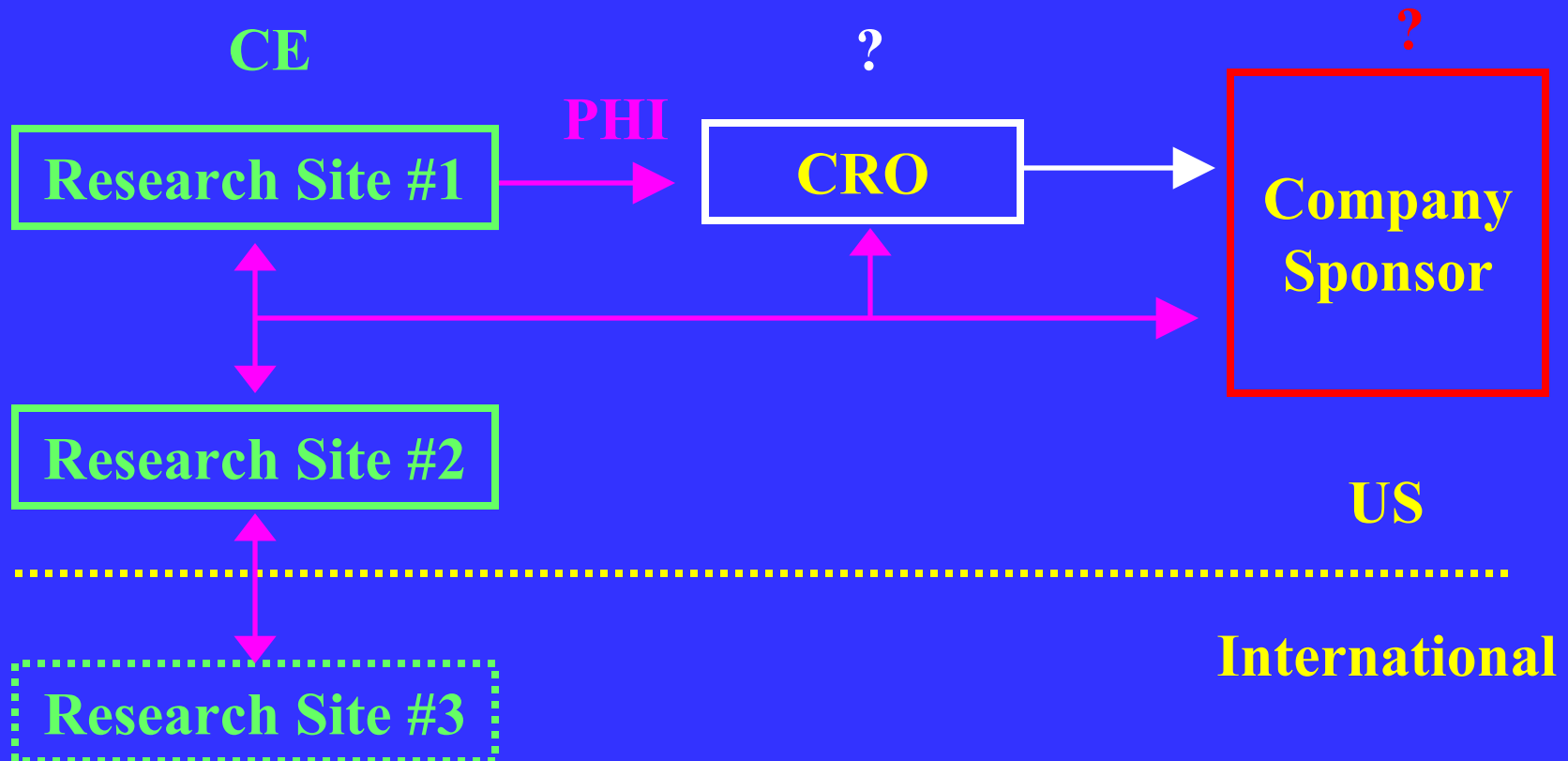
# Does HIPAA Apply?

---

**Research + CE + PHI = HIPAA  
Authorization**

- 1. Is it “research”?**
- 2. Is a “covered entity” involved?**
- 3. Is it “PHI”?**

# Typical Clinical Research Paradigm: How Will HIPAA Affect Sponsors?



# How Will HIPAA Affect Sponsors?

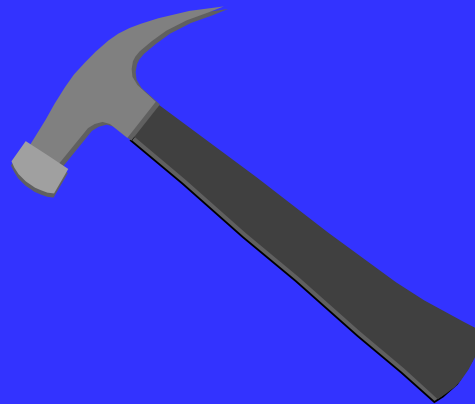
---

- **Affect on research paradigm**
  - **Sponsor must ensure a viable business model for clinical research**
  - **Map PHI from source to all necessary recipients (CRO, sponsor, FDA)**
  - **State and international privacy laws**
- **Direct affect on sponsor**
  - **Protocol modifications (screening, recruitment, informed consent form + authorization)**
  - **Contracts with other entities**
  - **Exposure to liability**

# How Will HIPAA Affect Sponsors?

---

**HIPAA will increase the liability risk for failure to protect privacy in medical research**





# HIPAA's Enforcement Provisions

---

## Who is subject to HIPAA's penalties?

- Any “person” who
- *Obtains* or discloses PHI in violation of HIPAA

## ● Civil penalty

- \$100 each violation, up to \$25,000/person/year

## ● Criminal Penalties

- **Knowingly:** ≤ \$50,000, 1 yr. jail
- **False pretenses:** ≤ 100,000, 5 yrs. jail
- **With intent to sell, transfer, or use for commercial advantage or personal gain:** ≤ \$250,000, 10 yrs. jail<sub>9</sub>

# Does HIPAA Apply?

---

**Research + CE + PHI = HIPAA  
Authorization**

- 1. Is it “research”?**
- 2. Is a “covered entity” involved?**
- 3. Is it “PHI”?**

# What is “Research”?

---

- **HIPAA = Common Rule**
- **Any *systematic* investigation,**
- **Designed to develop or contribute to *generalizable* knowledge (not just for knowledge or treatment of that subject) and**
- **Involves *human* subjects**
  - **HIPAA: applies to living and *deceased* persons**
  - **Common Rule and FDA regulations: apply only to “living” persons**

# What is “Research”?

---

- **Protocol development**
- **Development of research registries or databases**
  - **OHRP: Development of a repository or database for future research purposes is research.**  
<http://ohrp.osophs.dhhs.gov/humansubjects/guidance/reposit.htm>.
  - **HHS: “[T]he development of research repositories and databases for future research is considered research for purposes of the Privacy Rule.”** (Preamble to 8/14/02 final Privacy Rule)
- **Subject recruitment**
  - **HHS: subject recruitment is research – not marketing or health care operations** (preamble to 8/14/02 final Privacy Rule)
  - **Common Rule: Recruitment ads must be reviewed and approved by IRB** ( part of informed consent process)

# What Is Research?

---

- **Feasibility studies**
- **Subject screening**
- **Subject recruitment**
- **Subject enrollment and creating new PHI**
- **Use of existing PHI in databases, medical records, etc**

**Research + CE + PHI = HIPAA  
Authorization**

# Does HIPAA Apply?

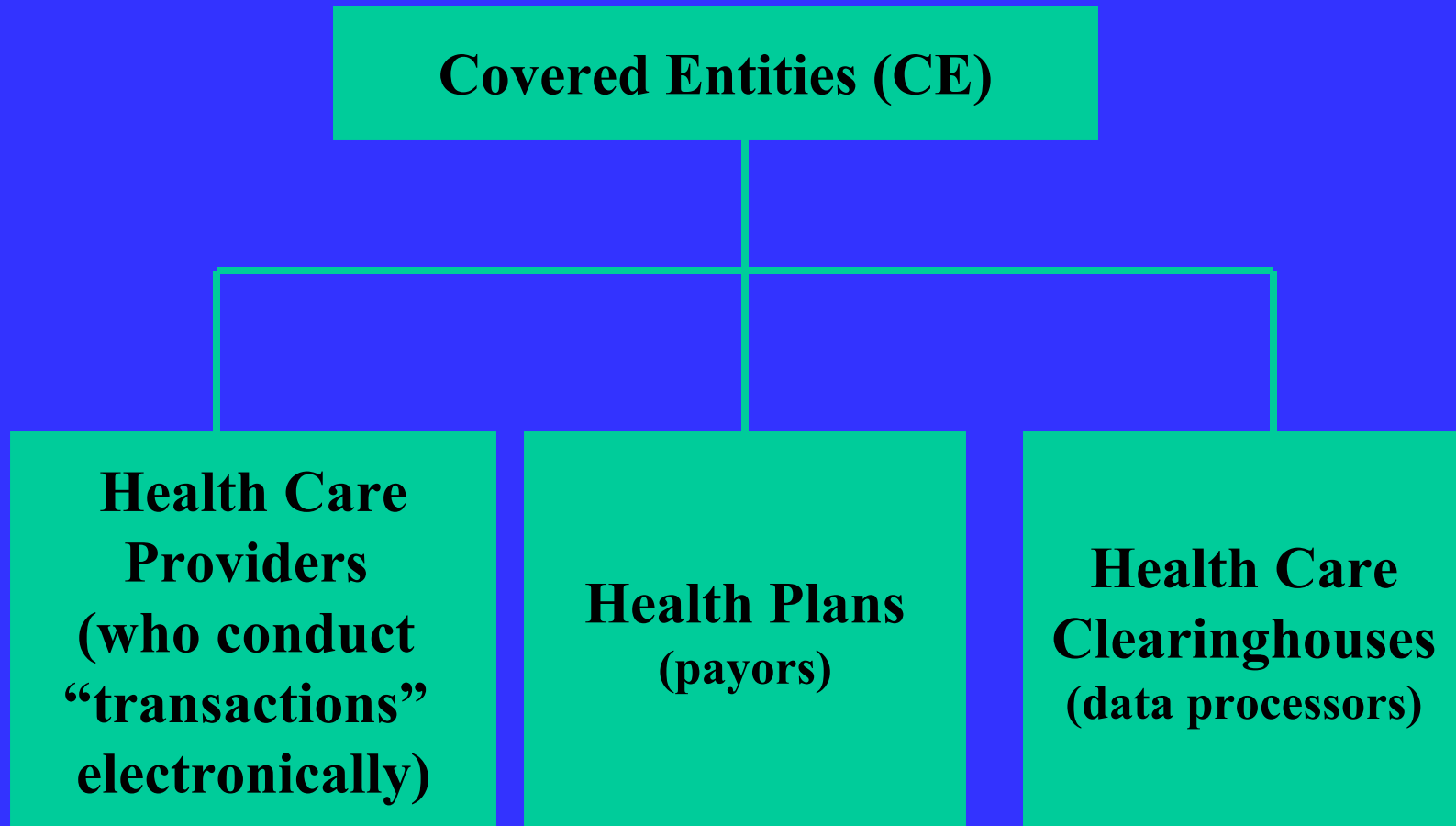
---

**Research + CE + PHI = HIPAA  
Authorization**

- 1. Is it “research”?**
- 2. Is a “covered entity” involved?**
- 3. Is it “PHI”?**

# Who Is a “Covered Entity”?

---



# Covered Entities: Health Care Providers

---

- **Furnish or provide, bill or receive payment**
- **For “health care”**
  - **Care, services or *supplies***
  - **Includes**
    - **Direct providers (physicians, nurses, social workers, pharmacists, etc.)**
    - **Indirect providers (*pharmaceutical companies, DME suppliers, etc.*)**
  - **Even if provided only in clinical trials**
- **And electronically transmits health information for a HIPAA “transaction” (billing/admin. for health care)**

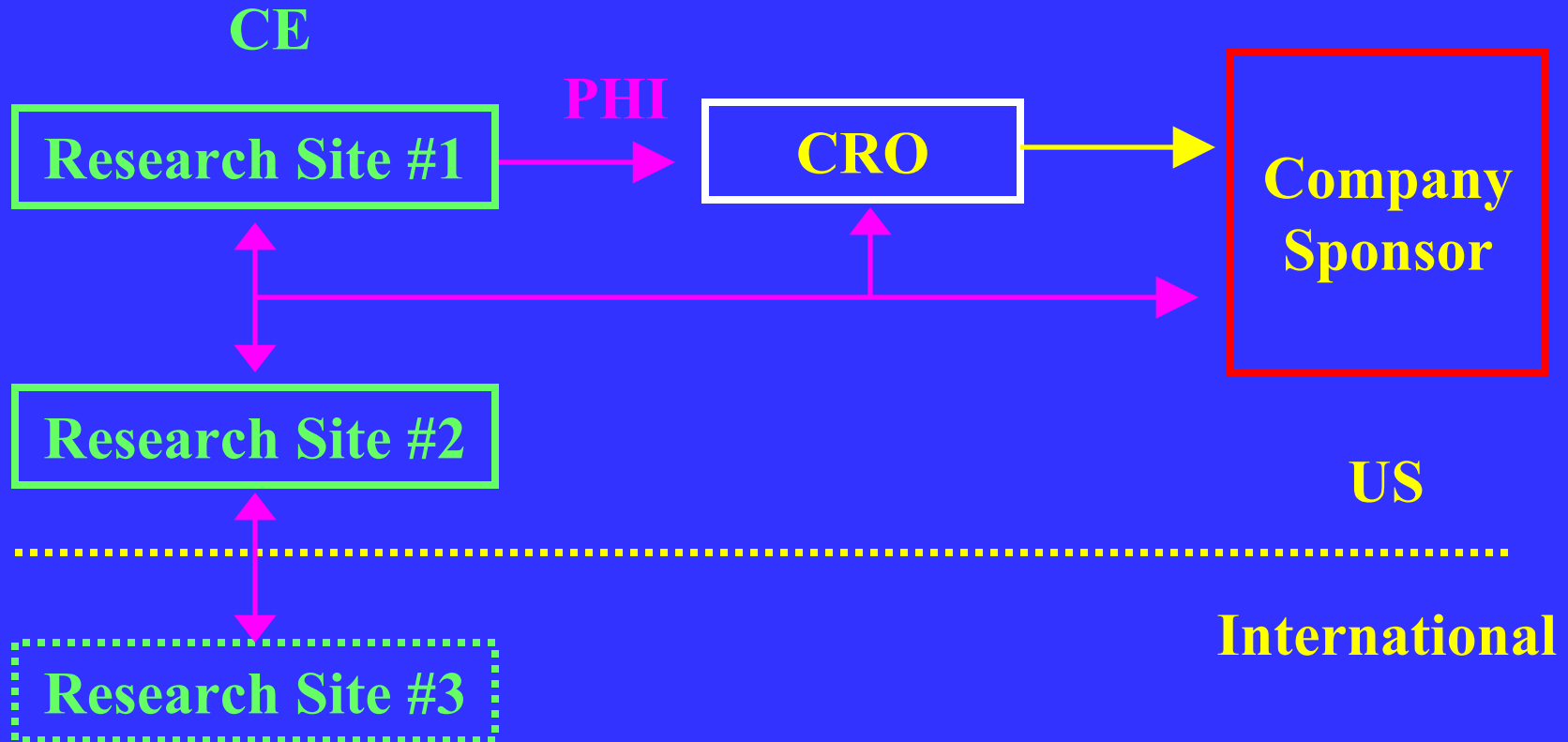


# Who is a Covered Entity?

---

- **Physician/researcher? Yes**
  - **HIPAA will affect use/disclosure of PHI for any research activity (subject screening, recruitment, research)**
- **Sponsor? Maybe but usually no**
  - **May be a health care provider (conduct in-house clinical trials, in-house clinics, provide supplies/services for clinical trials)**
- **CRO? Maybe but usually no.**

# Disclosure of PHI by the Covered Entity – Follow the PHI



**Research + CE + PHI = Authorization**

# Does HIPAA Apply?

---

**Research + CE + PHI = HIPAA  
Authorization**

- 1. Is it “research”?**
- 2. Is a “covered entity” involved?**
- 3. Is it “PHI”?**

# What is PHI?

---

- **Individually *identifiable* health information (IIHI)**
- **Created or received**
- **By a covered entity**

# Is it “Health Information”?

---

- Any oral or recorded information
- That relates to an individual’s past, present, or future:
  - Physical or mental health or condition,
  - Health care, or
  - Payment for health care
- Includes *demographic* data

# Is the Health Information “Identifiable”?

---

- **Identifiable**
  - Identifies an individual, or
  - There is a *reasonable basis* to believe it can be used to identify an individual
    - ❖ Includes *coded* health information

# Use or Disclosure of *Coded* PHI

---

- A covered entity may assign a code for re-identification (“re-identification code”), provided
  - Derivation: The code is *not derived from or related to information about the individual* and cannot be used to identify the individual; AND
  - Security: The covered entity *does not use or disclose the code* or other means for re-identification.
- Disclosure of a code or other means of re-identifying PHI or de-identified data constitutes disclosure of PHI

# What is *Not* PHI?

---

- De-identified data
- Limited data set



# “De-identified” Data

---

- **Methods:**
  - **Safe harbor: 18 direct identifiers are removed, or**
  - **Statistically de-identified**
- **And covered entity has *no actual knowledge* that the individual can be re-identified**

# Safe Harbor De-identification: Remove 18 Identifiers

---

- **Names** and ages  $\geq 89$  yrs (but *can* express in months, days, hrs)
- All dates (except year) directly related to an individual
- **Addresses:** geographic subdivisions smaller than a state, email, URLs, WWW, internet protocol address
- **Numbers:** telephone, and fax, social security, medical record, health plan, account, certificate/license numbers
- Vehicle or device identifiers and serial numbers
- Biometric identifiers (finger, voice prints), full face photos
- Any other unique identifying number, characteristic, or derived code (catchall)

# Limited Data Set (LDS)

---

- Excludes 15/18 direct ‘safe harbor’ identifiers
- Includes:
  - Dates (birth, death, admission, discharge)
  - Addresses (town/city, state, 5 digit zip code)  
*except* street address
  - Re-identification code

# Use and Disclosure of Limited Data Set

---

- **Authorization *not* required by covered entity:**
  - **To use LDS for research, public health or health care operations**
  - **To use PHI to create LDS**
- **Disclosure to third party requires a data use agreement**
  - **Minimum necessary rule applies**

# Disclosure of Limited Data Set: Data Use Agreements

---

- Permitted uses (research, public health, HCO)
- Who is permitted to use or receive the LDS
- Recipient responsibilities:
  - To *not* use LDS to contact individuals (may not use for recruitment) or identify the information
  - Report to CE unpermitted uses/disclosures of “which it is aware”
  - Use appropriate safeguards to comply with data use agreement
  - Ensure downstream compliance with agents & subcontractors

# HIPAA's Privacy Rule For Research

---

- **Research + CE + PHI = Authorization**
- **Exceptions:**
  - **Qualifies for a waiver of authorization**
  - **An exception applies**
  - **Disclosure to a business associate**
  - **Permitted disclosures**

# Criteria for Waivers or Alterations of Authorizations

---

1. The use/disclosure of PHI involves *no more than minimal risk* to the PRIVACY of the individual
  - Additional criteria
2. The research could not practicably be conducted without the alteration or waiver
3. The research could not practicably be conducted without access to and use of PHI

# Criteria for Waivers or Alterations of Authorizations

---

- Adequate plan to *protect the identifiers* from improper use and disclosure;
- Adequate plan to *destroy the identifiers* at the earliest opportunity; and
- Adequate written *assurances* that the PHI will not be reused or disclosed to any other person or entity unless authorized



# Waiver or Alteration of Authorization Requirements For Research

---

- **Who must approve the waiver/alteration?**
  - **Institutional Review Board (IRB), or**
  - **Privacy board**
- **Waiver or alteration must be requested and approval documented in writing**

# Exceptions to the General Rule – When is an Authorization *Not* Required?

---

- Research qualifies for a waiver of authorization
- An exception applies (n = 2)
- Disclosure to a business associate
- Permitted disclosures

# Exceptions to Authorization Requirements

---

## 1. Reviews *preparatory* to research

- Use/disclosure of PHI is solely to prepare a *research protocol* or for a similar purpose (preparatory to research),
- PHI may not be removed from the covered entity, and
- PHI is necessary for research purposes

## 2. Research on PHI from *decedents*

# Reviews Preparatory to Research: Process

---

- Covered entity must obtain a “representation” from the researcher that
  - PHI will not be removed from CE’s site,
  - PHI will be used solely for protocol development or equivalent, and
  - PHI is necessary for research
- No IRB/privacy board approval required
- Who processes the representations at the CE?

# Exceptions to the General Rule – When is an Authorization *Not* Required?

---

- Research qualifies for a waiver of authorization
- An exception applies (n = 2)
- Disclosure to a business associate
- Permitted disclosures

# Who is a “Business Associate”?

---

- Uses a covered entity’s PHI
- To perform a specified function or service *on behalf of* or *for* a covered entity
- With whom the covered entity has a written business associate contract
- Can’t be part of the covered entity’s workforce

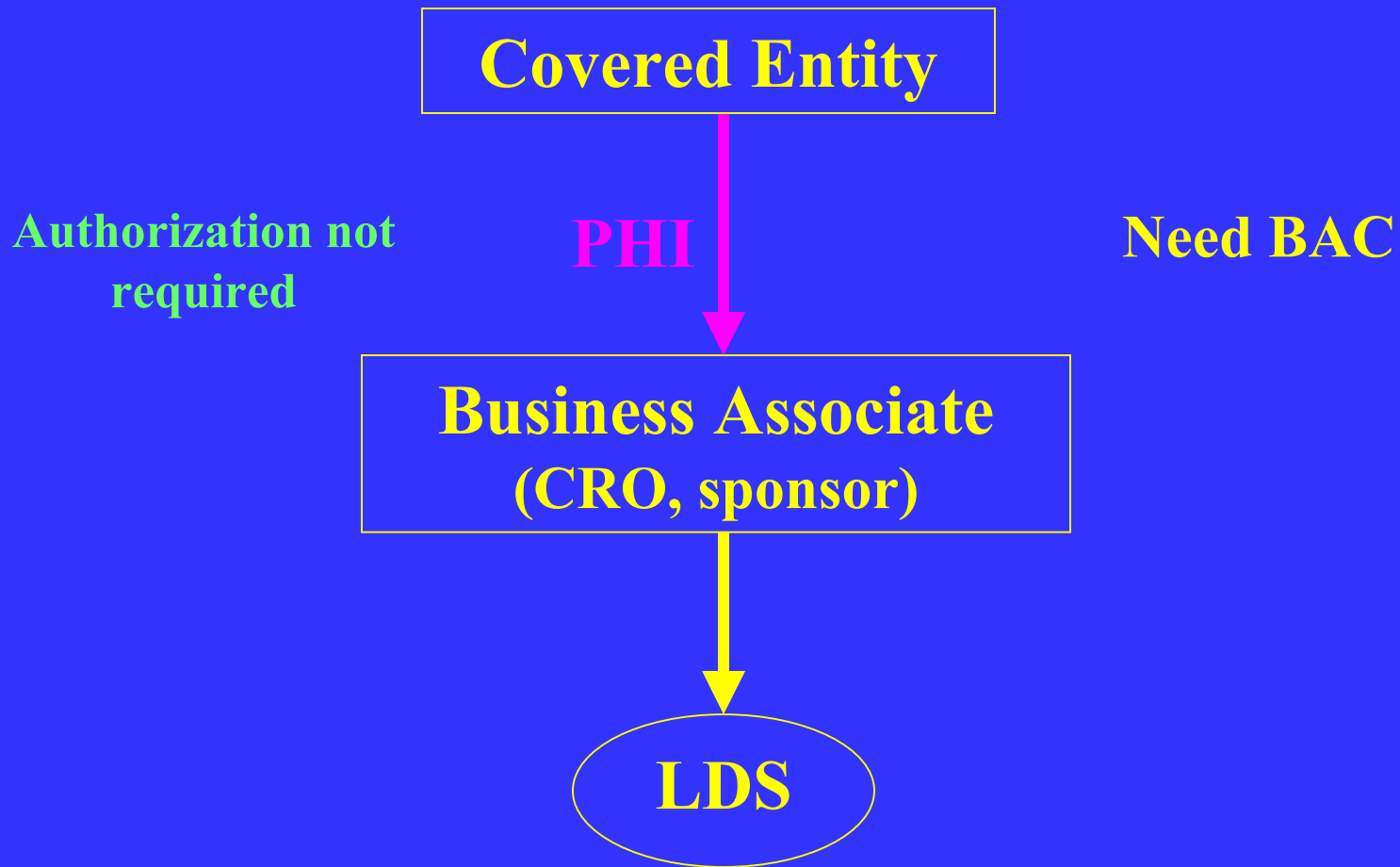
# Who is a “Business Associate”?

---

- Disclosure of PHI to a third party for the purpose of creating:
  - De-identified data
  - LDS
- Creates a business associate relationship
  - “[A] covered entity may engage a business associate to create a limited data set, in the same way it can use a business associate to create de-identified data. As with de-identified data, a business associate relationship arises even if the limited data set is not being created for the covered entity’s own use.” (Preamble to final Privacy Rule, 8/14/02)

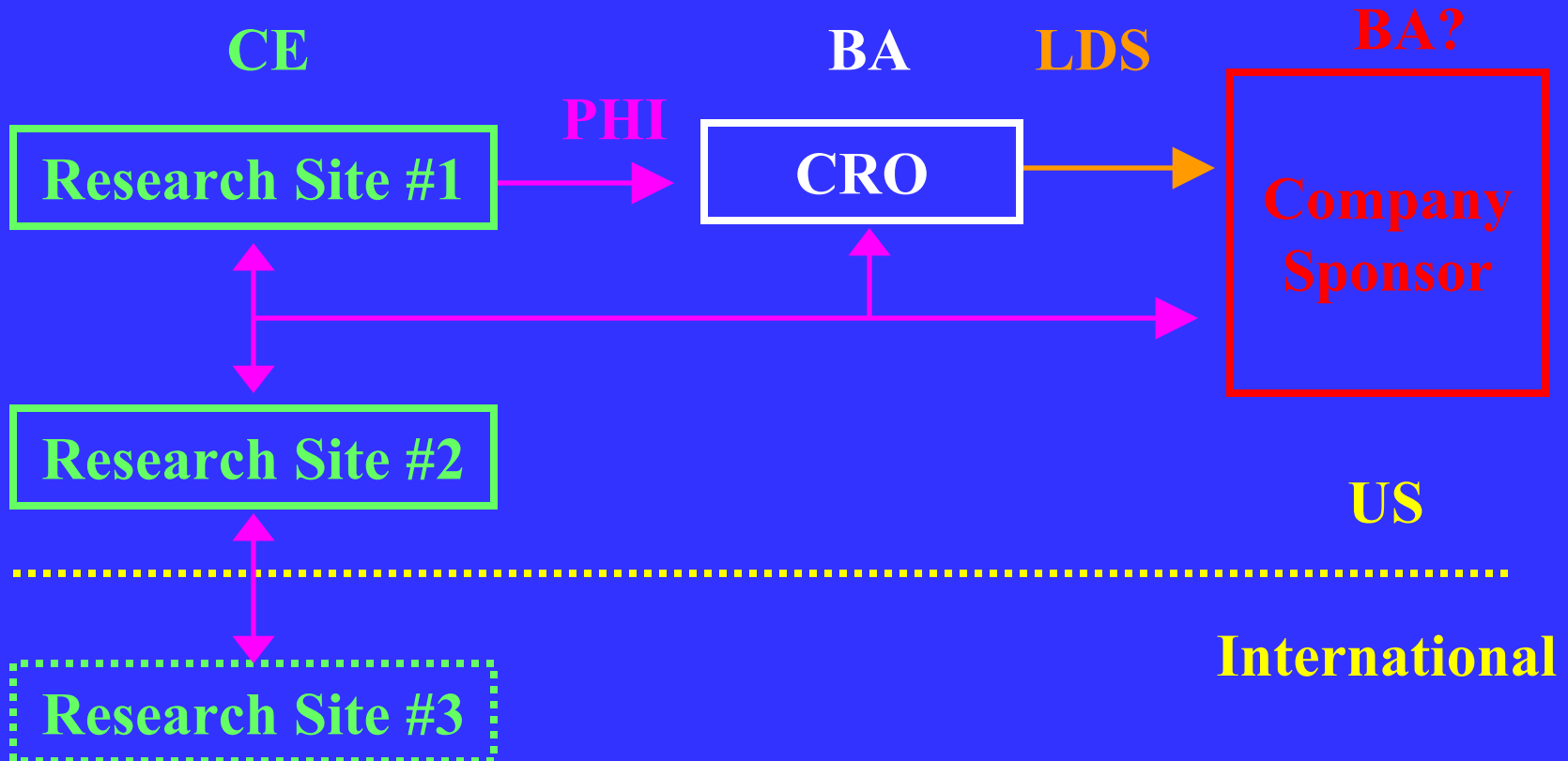
# Disclosure of PHI to Business Associate to *Create A Limited Data Set*

---





# Typical Clinical Research Paradigm: Who Is a Business Associate?



# Exceptions to the General Rule – When is an Authorization *Not* Required?

---

- Research qualifies for a waiver of authorization
- An exception applies (n = 2)
- Disclosure to a business associate
- Permitted disclosures

# Permitted Public Health Disclosures Under HIPAA: FDA Reporting

---

- **CEs may disclose PHI w/o authorization to:**
  - **Persons subject to FDA jurisdiction**
  - **“Person” includes companies (sponsors)**
- **With respect to an FDA-regulated product**
- **Regarding the safety, effectiveness or quality of the product**
  - **Includes: Adverse events, device tracking, product recalls, lookbacks, post-marketing surveillance**
  - **Excludes: marketing**
- **Minimum necessary applies**

# Subject Screening and Recruitment Under HIPAA

---

## 1. Subject screening

- No subject contact
- Medical records review
- Screen databases or repositories

## 2. Subject recruitment

- Subject contact
- Non-targeted advertising
  - Passive (one-way flow of information)
  - Interactive (two-way flow of information)
- Targeted contacts (phone calls, letters, emails, physician-patient contact)

# Subject Screening

---

- **Research + CE + PHI = Authorization**
- **Does an exception apply? Yes**
- **Reviews preparatory to research**
  - **Allows any “researcher” (sponsor, CRO, CE, BA) to look at PHI at CE’s site**
  - **Limitations**
    - ❖ **PHI may not be *removed* from covered entity’s site**
      - ◆ **No hard copy or electronic copy**
      - ◆ **No remote access (email, internet)**
    - ❖ **PHI may not be used to *contact* subjects**

# Reviews Preparatory to Research: May *Not* be Used to Recruit Subjects

---

**NPRM, March 2002:**

**“Commenters expressed concern and confusion as to how researchers would be able to recruit research subjects when the Privacy Rule does not permit [PHI] to be removed from the covered entity’s premises during reviews preparatory to research.”**

**“The Department clarifies that the Privacy Rule’s provisions for IRB or Privacy Board waiver of authorization are intended to encompass a partial waiver of authorization for the purposes of allowing a researcher to obtain [PHI] necessary to recruit potential research participants.”**

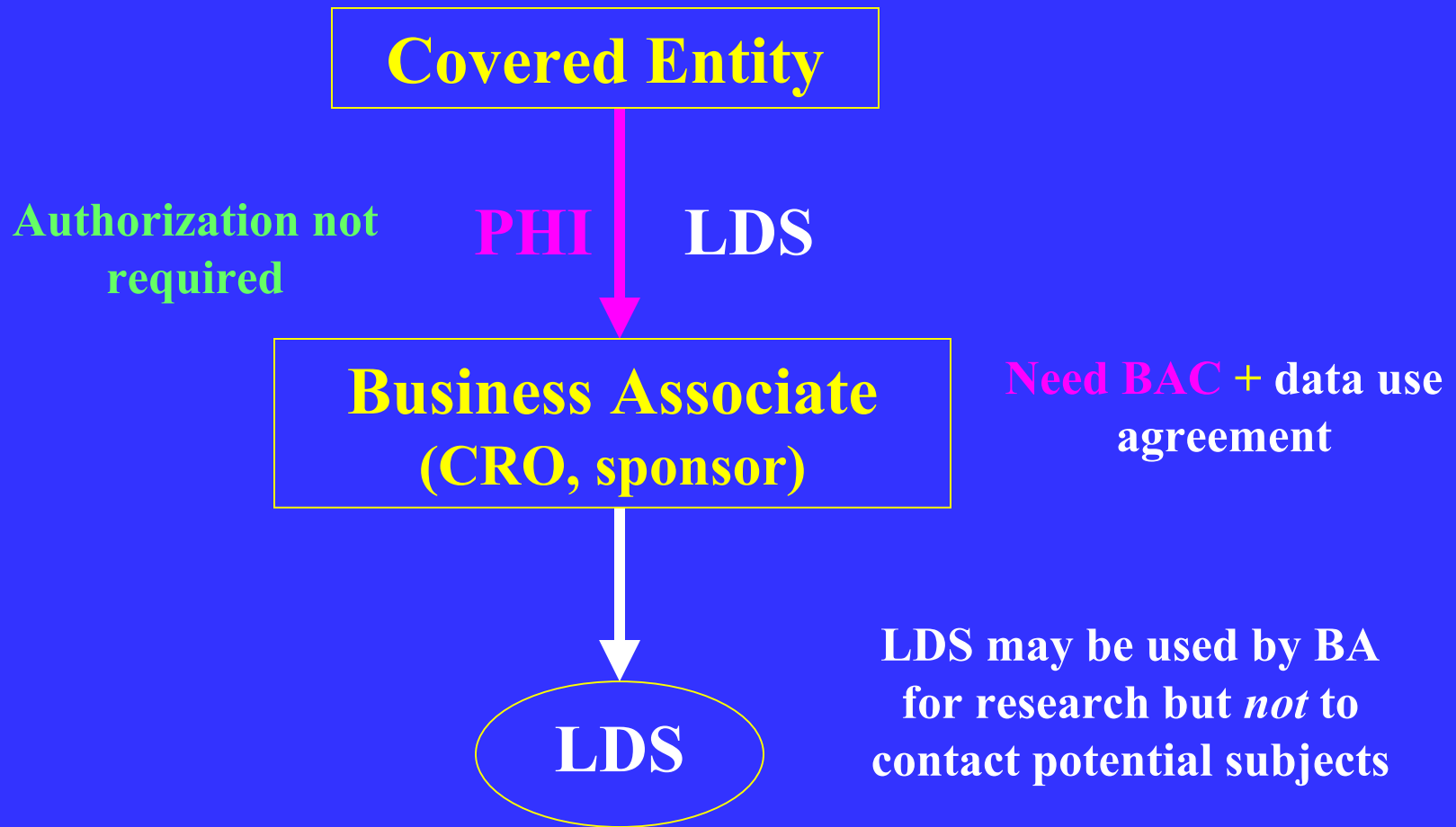
# Reviews Preparatory to Research: May *Not* be Used to Recruit Subjects

---

**NPRM, March 2002:**

**“For example, even if an IRB does not waive informed consent and individual authorization for the study itself, it may waive such authorization to permit the disclosure of protected health information to a researcher as necessary for the researcher to be able to contact and recruit individuals as potential research subjects.”**

# Use of Limited Data Set for Subject Screening





# Mechanisms For Subject Screening

---

- **Reviews preparatory to research**
  - **Need representation from researcher**
  - **PHI may not be removed from site**
- **Limited data set**
  - **Covered entity may *use* w/o authorization**
  - **Covered entity may *disclose* with data use agreement**
  - **Covered entity may disclose PHI to business associate (with BAC) to create LDS**

# Subject Recruitment/Contact

---

- **Non-targeted contacts**
  - **General advertising (TV, radio, internet, newspaper, bulletin boards, etc.)**
    - ❖ **Passive ads**
    - ❖ **Interactive ads**
- **Targeted contacts**
  - **Subject-specific contacts (phone calls, letters, emails)**
    - ❖ **By sponsor**
    - ❖ **By physician/researcher**
  - **Patient-MD interaction**

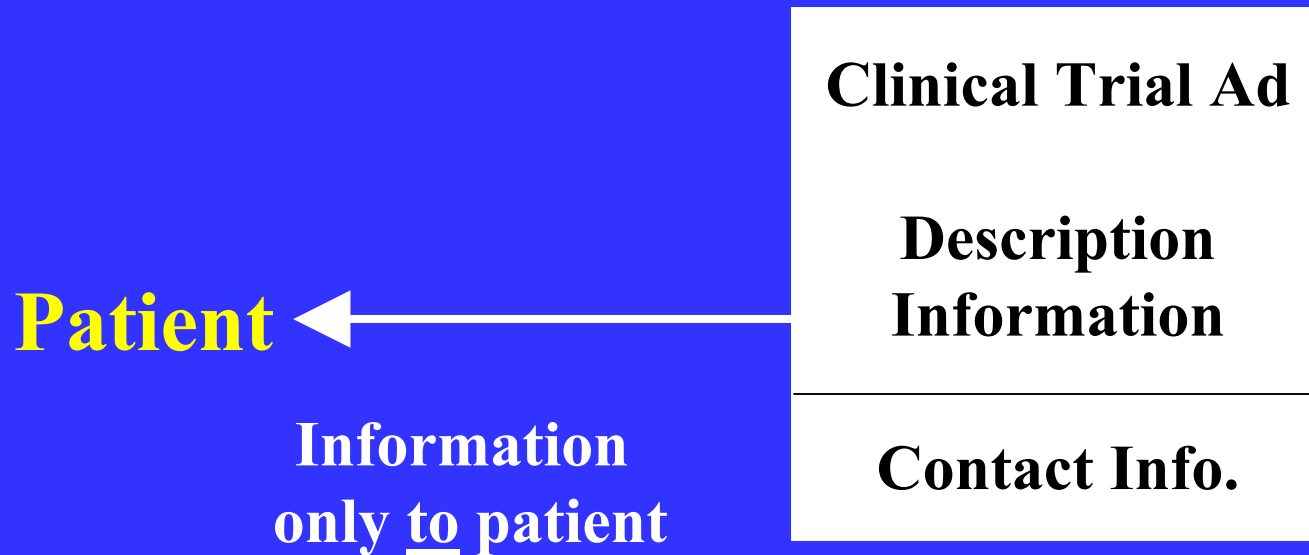
# Subject Recruitment/Contact

---

- **May *not* use LDS to contact subjects**
- **May *not* do under “Reviews Preparatory to Research” exception (not protocol development)**
- **Must either have:**
  - **Authorization (e.g., obtained in previous study), or**
  - **Waiver of authorization**
    - ❖ **Waiver for subject recruitment = “partial waiver” of authorization (preamble to NPRM)**

# Subject Recruitment: General 'Passive' Advertising

---



# Subject Recruitment: General 'Interactive' Advertising

Is source a  
covered entity?

Is recipient a  
covered entity?

**Patient**  
**or**  
**Physician**

PHI?

**Clinical Trial Website**

**Description  
Information**

**Patient Information  
(Name, phone, email,  
other)**

**Cookies/Clickstream data  
DoubleClick Info/3Ps**

# Subject Recruitment: Use of Databases or Repositories

---

- **Development of database/repository for recruitment = research**
- **Covered entity may use PHI or disclose PHI to third party for recruitment *only* with:**
  - **Prior authorization**
  - **Prior legal permission (transition provisions)**
  - **Documented waiver of authorization**

# Subject Recruitment By Treating Physician

---

- **Question: May a covered health care provider use a patient's PHI to discuss a clinical trial with a patient?**
- **Answer: Yes**
  - **Disclosure of PHI to an "individual" is permitted under § 164.502(a)(1)(i)**
    - ❖ **"Individual" is the subject of the PHI**
    - ❖ **Authorization or waiver not required**
    - ❖ **"[C]overed health care providers and patients may continue to discuss the option of enrolling in a clinical trial without patient authorization [or waiver]." (Preamble to final Privacy Rule.)**

# Use or Disclosure of PHI by Covered Entity for Recruitment

---

- *Use of PHI*

- Use of PHI obtained through TPO (not research): no authorization or waiver
- Use of PHI in research database: need authorization, waiver or prior legal permission (transition/grandfather provisions)

- *Disclosure of PHI*

- Need: authorization, waiver or prior legal permission (transition provisions)

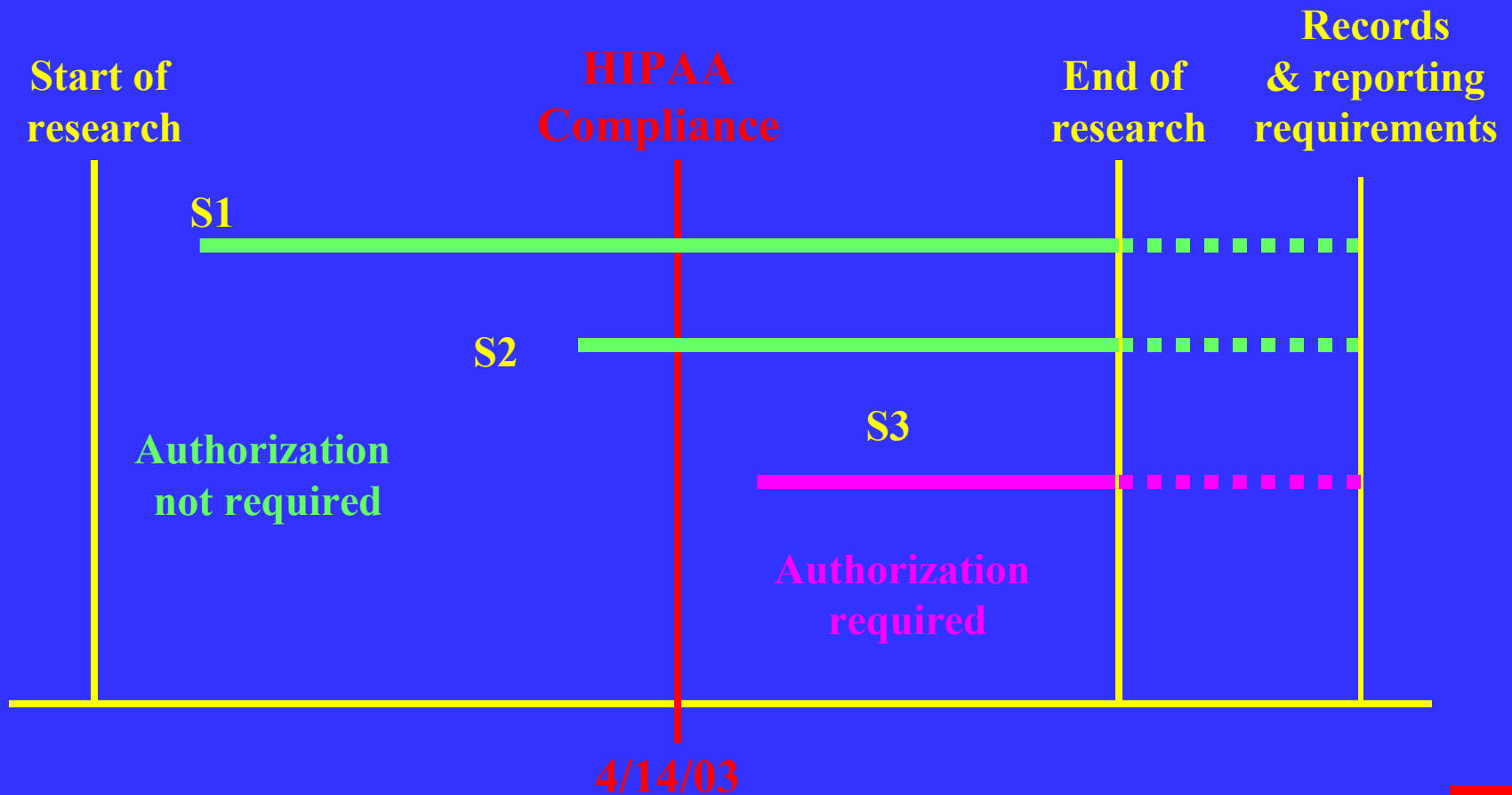


# HIPAA's Grandfather Provisions

---

- Covered entity may use/disclose PHI
- That it created or received before or *after* the HIPAA compliance date (4/14/03)
- For a research study
- IF the covered entity obtained either
  - Informed consent,
  - IRB-approved waiver of informed consent, or
  - Express legal permission
- *Before* the compliance date

# Application of HIPAA's Grandfather Provisions To On-Going Studies



# HIPAA Authorizations: Right To Revoke

---

- **Right to revoke at any time**
  - **Statement that individual may revoke in writing at any time unless the covered entity has acted “in reliance on” authorization**
- **CE may continue to use/disclose PHI collected before the revocation as needed “to preserve the integrity of the research study”**
  - **Does not apply to tissue**
- **Permitted uses/disclosures:**
  - **Accounting of subject’s withdrawal**
  - **Required reports to FDA or other agencies**
  - **To investigate scientific misconduct allegations**

# Multi-site Studies

---

- **State laws**
  - HIPAA preempts state laws that are contrary to and less stringent than HIPAA
  - Need to determine the floor of privacy protection in *each* state (preemption analysis)
  - General medical confidentiality laws
    - ❖ Research exceptions (variable)
  - Specific confidentiality laws (*e.g.*, HIV/AIDS, mental illness, genetic privacy acts)
- **International laws**

# Conducting Clinical Trials Under HIPAA - Implications For Sponsors

---

- **New procedures**
  - **Feasibility studies and subject screening**
    - ❖ **Representations to CE**
    - ❖ **Minimum necessary rule applies**
  - **Subject recruitment**
    - ❖ **Partial waivers - IRB/privacy board review and approval**
    - ❖ **Protocol revisions - recruitment and enrollment**
    - ❖ **Interactive websites**

# Conducting Clinical Trials Under HIPAA - Implications For Sponsors

---

- **Revise informed consent form**
  - **Add 8 authorization elements to model informed consent forms (expiration date/event)**
- **Revise clinical trial agreements**
- **Track data use agreements (LDS)**
- **State preemption analyses**
- **Analysis of international laws**
- **Business associate responsibilities**
  - **Business associate contracts**
  - **Track disclosures (to and from) for 6 years**
  - **Subject's right to access PHI**
  - **Subject's right to amend**

# Conducting Clinical Trials Under HIPAA - Implications For Sponsors

---

Questions?

