Research Compliance A: Effect of HIPAA On Research, Part II

Carol A. Pratt, Ph.D., JD

Davis Wright Tremaine LLP

Portland, OR

Seattle, Portland, San Francisco, Los Angeles,
Anchorage, HonoluluCharlotte

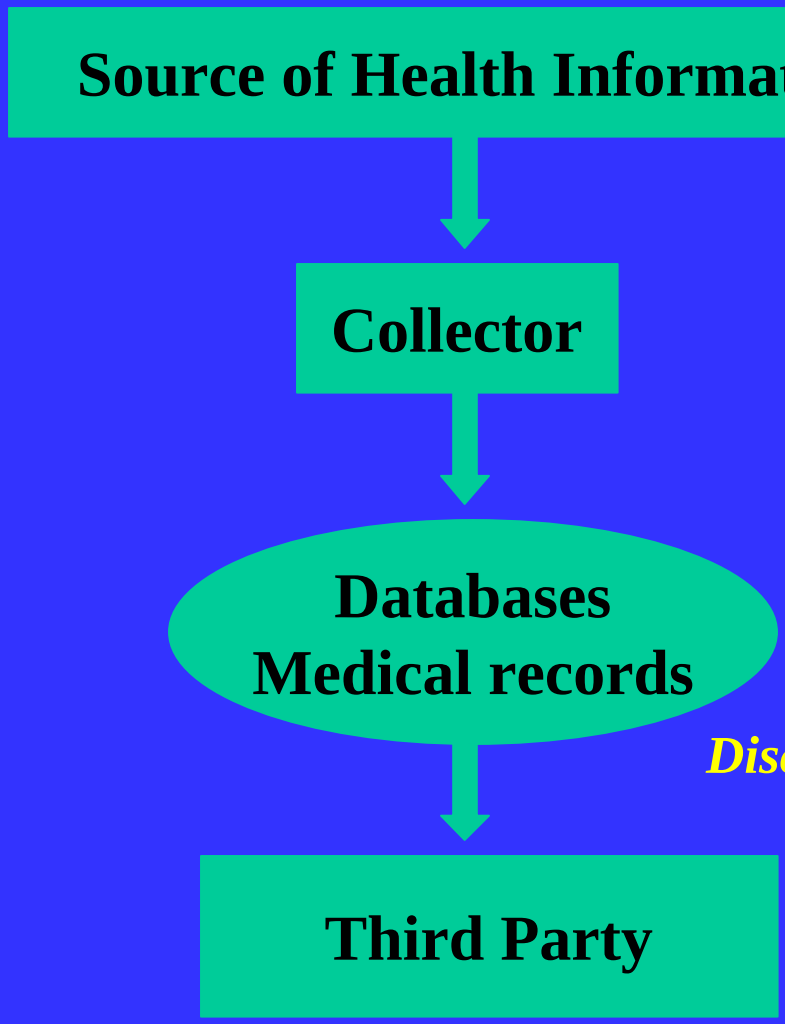
(503) 778-5279

carolpratt@dwt.com

HIPAA's Privacy Standard

- A covered entity may not use or disclose
- Protected health information (PHI)
- Without individual written *consent* for routine purposes, including:
  - Treatment, payment and health care operations
- Without written *authorization* for non-routine purposes
  - Includes research
  - Authorization requirement may be *waived* for some research purposes

HIPAA's Restrictions on "Use" or "Disclosure" of PHI



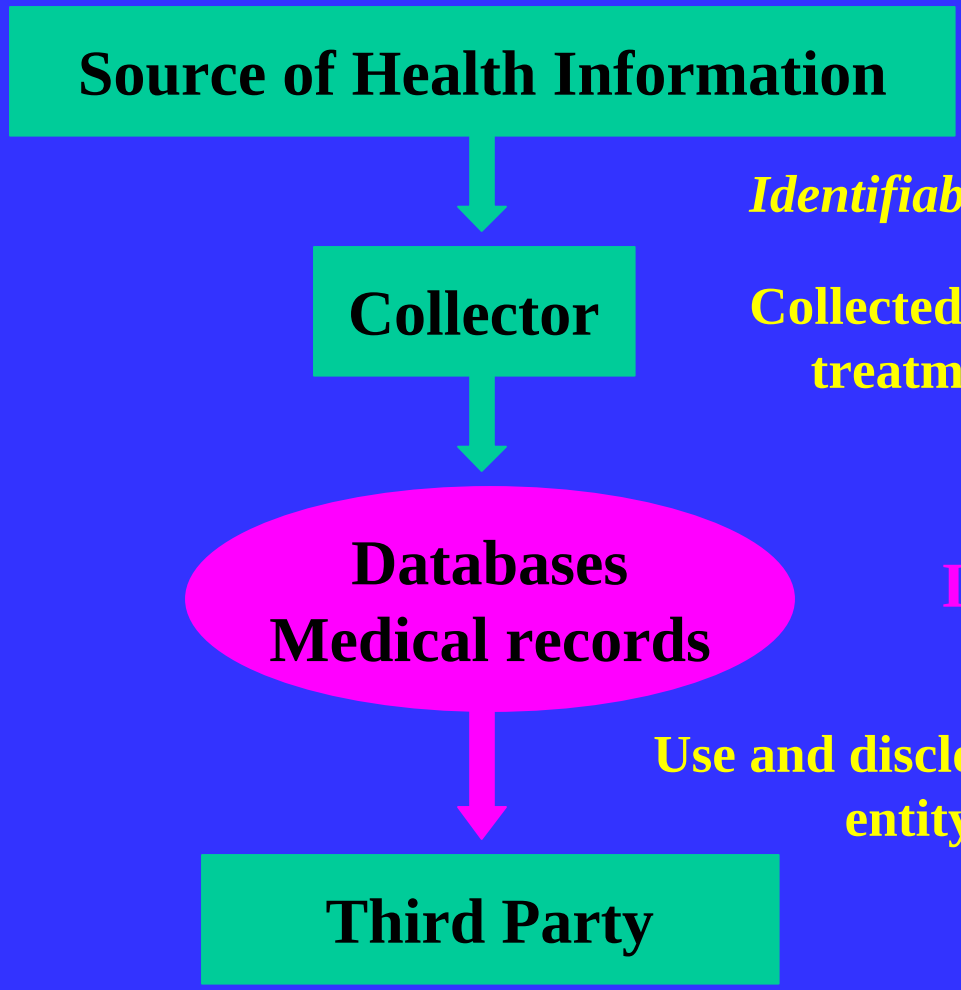
Use **of PHI includes analysis andutilization**

Disclosure **of PHI includes release, transfer, or providing access to PHI or code**

Use and Disclosure of PHI in Research

- **Research + Treatment**
  - **Clinical trials**
  - **Generate *new* PHI and use *existing* PHI**
  - **Use existing PHI to screen and recruit select populations of subjects**
- **Research**
  - **Retrospective studies of *existing* databases**
  - **Prospective collection of new data**
  - **Epidemiological research**
    - **Data: medical records, demographics, mortality data, specimen registries (*e.g.*, tumors), disease registries**

What is PHI?



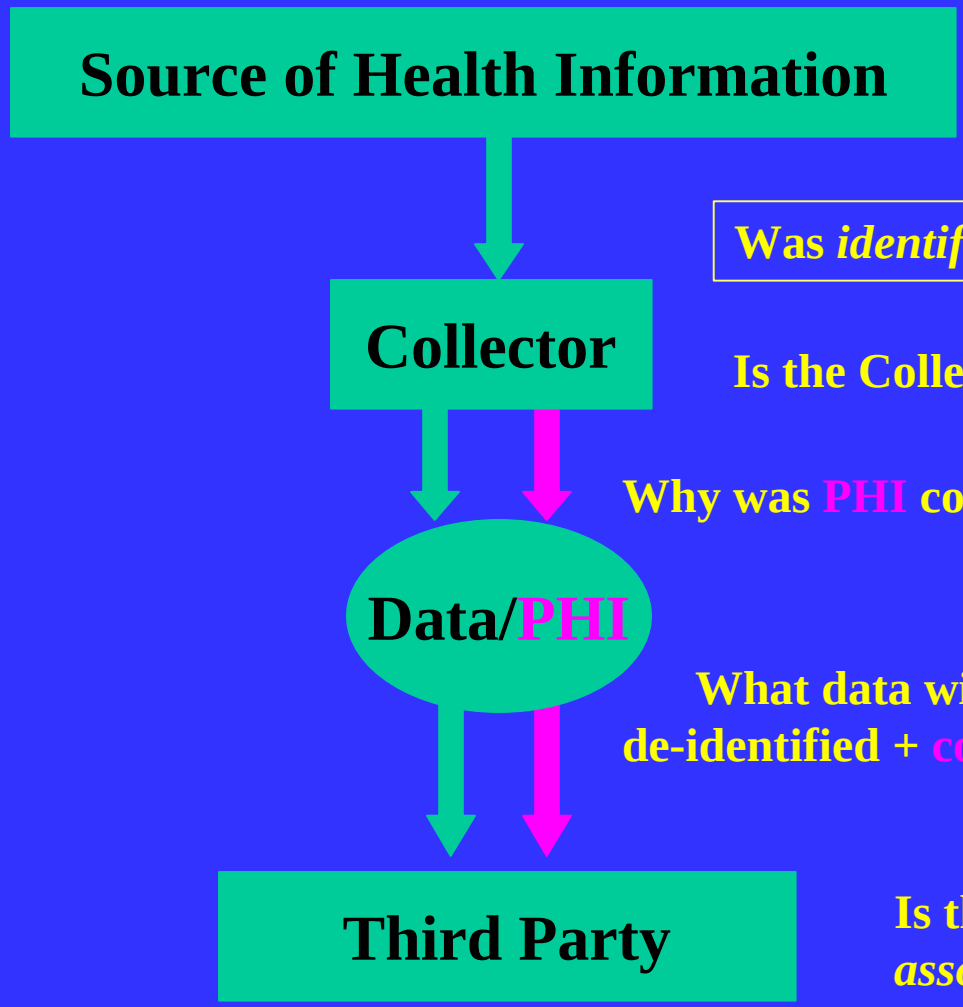
Identifiable health information

Collected by a *covered entity* for treatment and/or research

Is PHI

Use and disclosure of the PHI by the covered entity is regulated by HIPAA

Is Authorization Required?



Was *identifiable* health information collected?

Is the Collector a *covered entity*?

Why was PHI collected (Tx, research + Tx, research)?

What data will be disclosed (de-identified, de-identified + code, identifiable/coded, identified)?

Is the Third Party a *business associate* of the covered entity?

Was "Health Information" Collected?

- 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

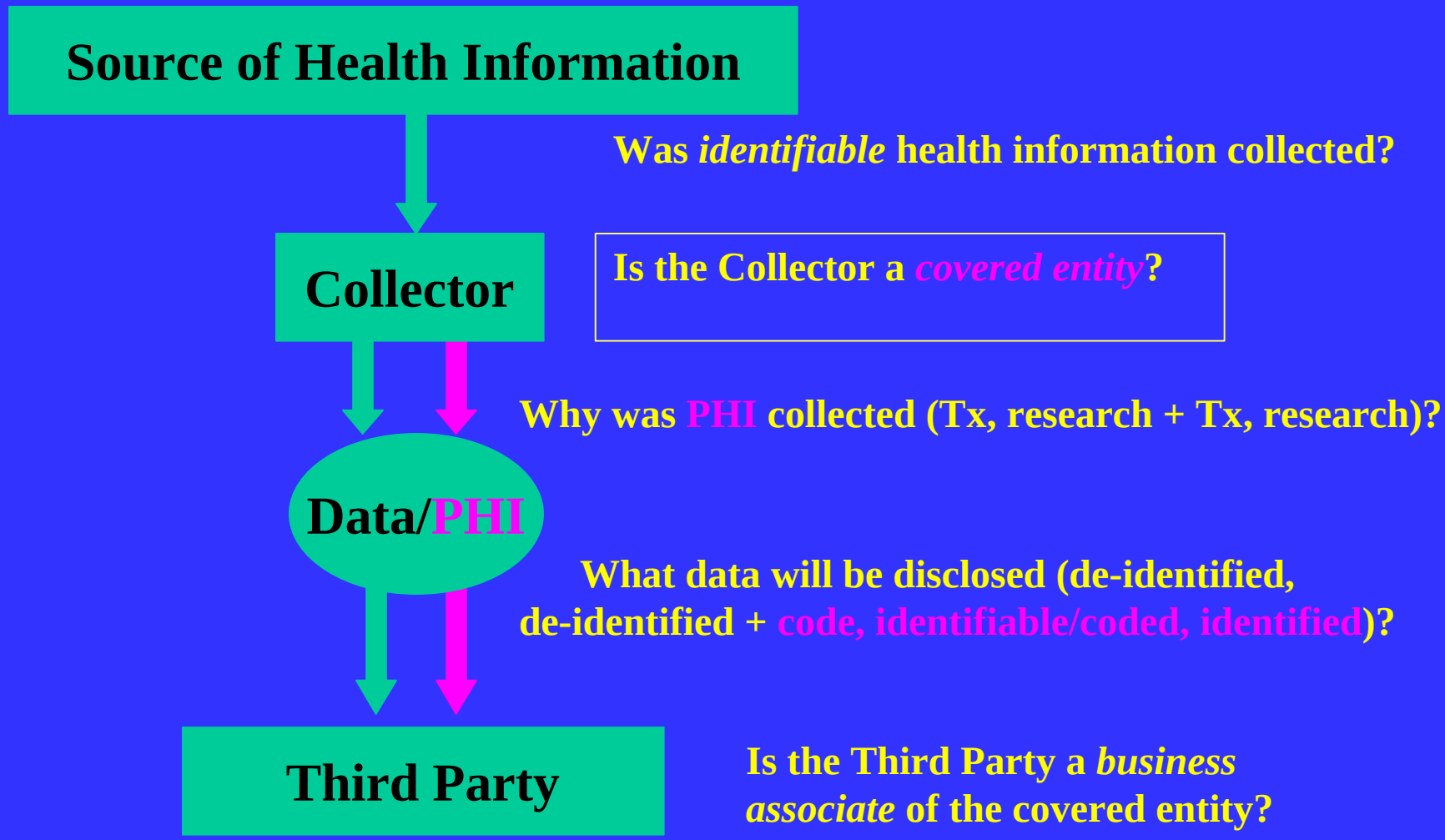
Is the Health Information *Identifiable*?

- **Identifiable**
  - **Identifies an individual, or**
  - **There is a *reasonable basis* to believe it can be used to identify an individual**
    - **Includes *coded* health information**
- **De-identified**
  - **HIPAA's 18 identifiers removed (§164.514(b)(2)(i))**
  - **Or statistically de-identified (§164.514(b)(1))**
  - **And covered entity has *no actual knowledge* that the Source can be reidentified**
- **Unidentifiable**
  - **No source identifiers were collected (anonymous)**
  - **Aggregated data**

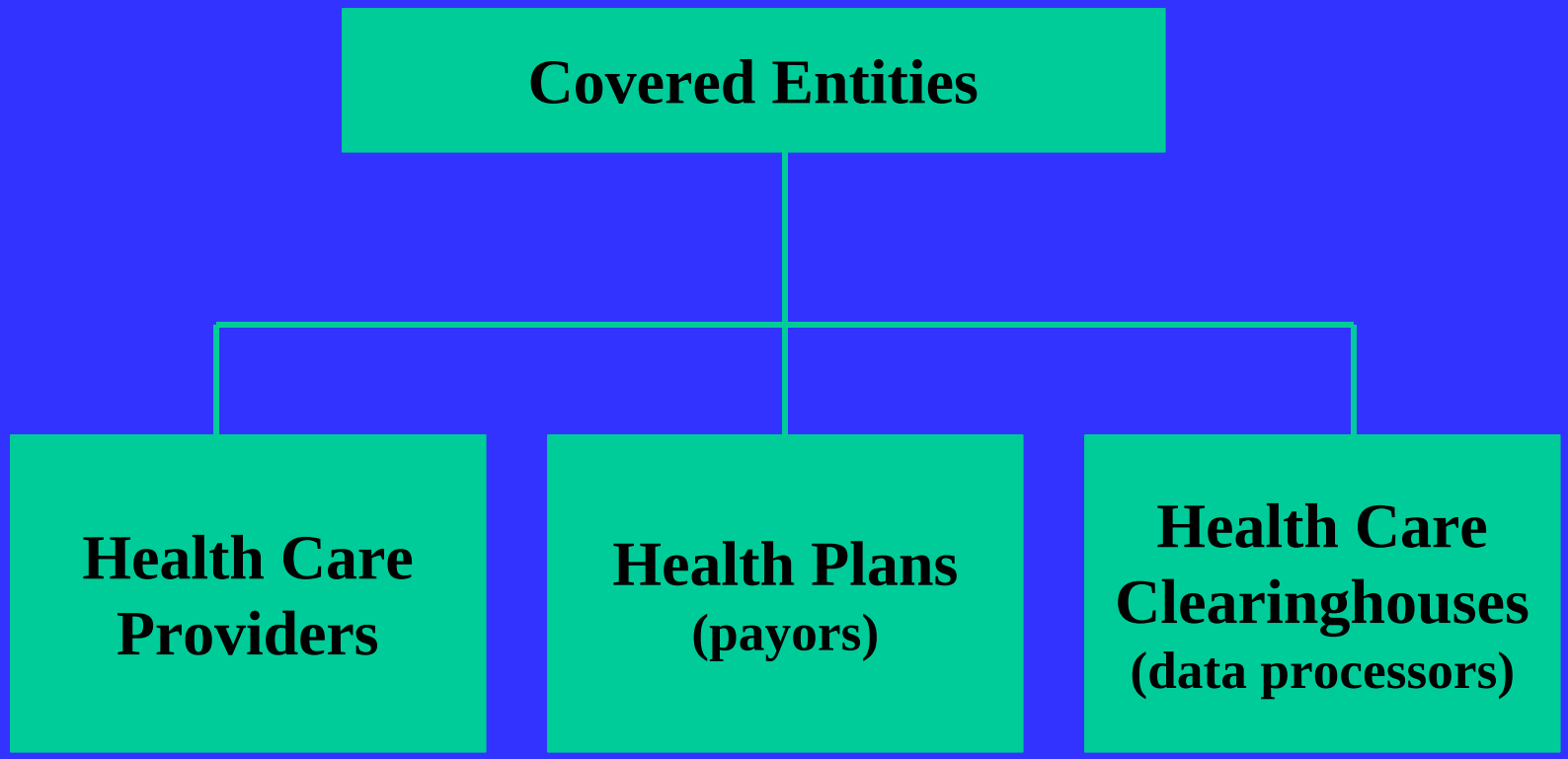
Use or Disclosure of Coded PHI

- **A CE may assign a code for re-identification, <u>provided</u>**
  - **<u>Derivation</u>: The code *is not derived from or related to information about the individual* and cannot be used to identify the individual; <u>AND</u>**
  - **<u>Security</u>: The covered entity *does not use or disclose the code* or other means for re-identification. § 164.514(c).**
- **Disclosure of a code or other means of reidentifying deidentified PHI *constitutes disclosure of PHI*. §164.502(d)(2)(i).**

Is Authorization Required?



Were the Data Collected By a *Covered Entity*?



Covered Entities: Health Care Providers

- **Individuals and facilities who provide health care, services or supplies related to the health of individuals**
  - **Diagnosis, treatment, rehabilitation, counseling, assessment for a physical or mental condition, or**
  - **Sale or dispensing prescription drugs or devices.**
- **And transmit health information in *electronic* form.**

Covered Entities: Health Care Providers

Includes:

- Individual providers (physicians, pharmacists, and other licensed health care practitioners)
- Facilities (hospitals, SNFs, rehabilitation facilities, home health agencies, hospice)
- On-line pharmacies

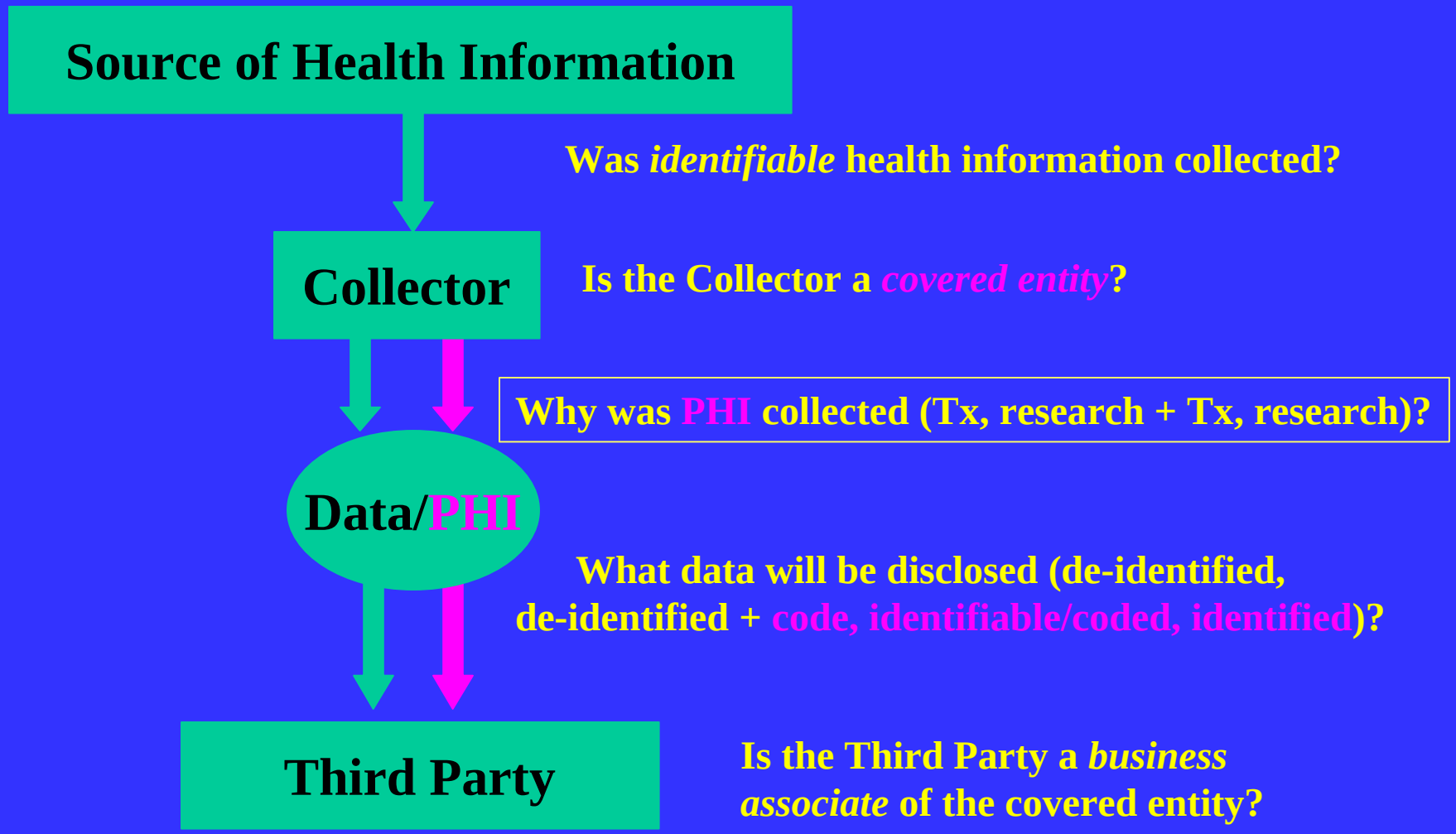
Does *not* include:

- Ph.D. researchers
- Tissue banks (procurement of human blood, tissue or organs)

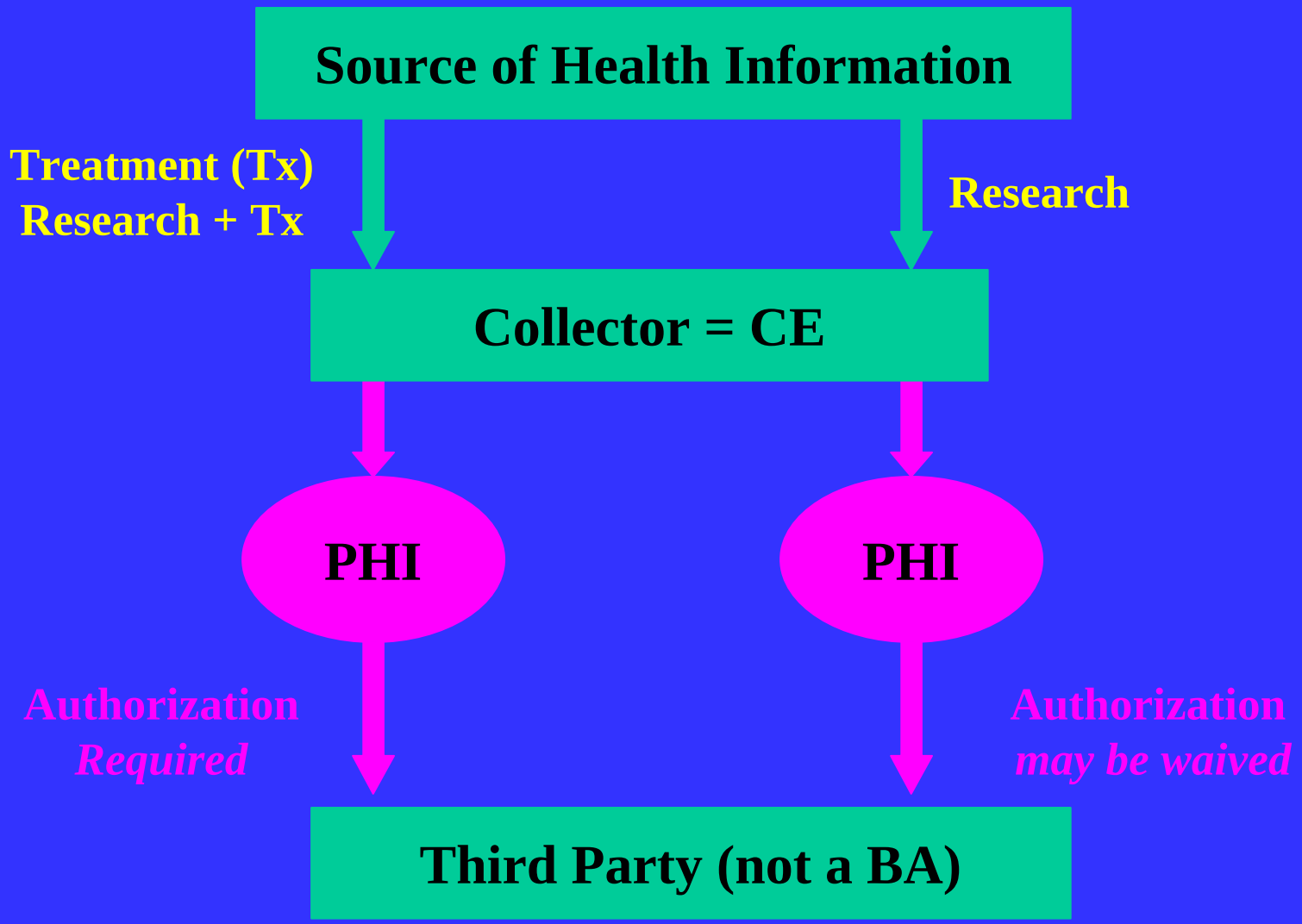
Were the data collected by a covered entity?

Are non “health care providers” who are employees of a covered entity and who collect PHI subject to HIPAA ?

Is Authorization Required?



Why Was PHI Collected?



Why Was PHI Collected?

- **Research: systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.**
  - **Same as DHHS (45 CFR 46.102(d)**
- **Treatment: the provision, coordination, or management of health care and related services by one or more health care providers, including:**
  - **coordination or management of health care by a health care provider with a third party;**
  - **consultation between health care providers relating to a patient; or**
  - **the referral of a patient for health care from one health care provider to another.**

Why Was PHI Collected?

- **Research that *includes treatment* (clinical trials) (§164.508(f)(1))**
  - **Written individual authorization is *required* for**
  - **PHI created, *in whole or in part*, for research + Tx (clinical trials).**
- **Research (§164.512(i)(f))**

  For all research *regardless of funding source* (§164.512(i)(1)):

  - **Authorization requirements may be *waived* or *altered* by an:**
    - **Institutional Review Board (IRB)**
    - **Privacy Board**
  - **Waiver not required for:**
    - **reviews preparatory to research**
    - **PHI from *deceased* persons**

Clinical Trials: Informed Consent and HIPAA Authorization

Will HIPAA affect informed consent for clinical trials?

- HIPAA's authorization requirements *exceed* those required by DHHS (45 CFR 46) or FDA (21 CFR 50, 56)
- HIPAA's authorization requirements *may* be added to informed consent forms (§164.508(f)(2))
- Clinical trials involving complex protocols (*e.g.*, cancer trials) may want to keep HIPAA authorization separate from informed consent forms

Authorizations For Clinical Trials

Core elements for authorization (§164.508(f)(1))

- ✓ Overlap with informed consent form
  - ✓ Plain language
  - • Specific, meaningful description of PHI (what data will be collected?)
  - ✓ Names or specific identification of persons (or classes of persons) authorized to use or disclose PHI
  - • Expiration date or event
  - • Statement that individual may revoke in writing <u>unless</u> the covered entity has acted in reliance of authorization
  - • Warning that redisclosure of disclosed PHI may be unprotected
  - ✓ Signature of individual and date
  - ✓ Copy to the individual

Authorizations for Clinical Trials

Requirements for covered entity to use/disclose its own PHI (§164.508(d):

- ✓ **Description of each *purpose* of the use or disclosure**
- **Statement that patient may:**
  - ➢ ***inspect* and *copy* the PHI**
  - ✓ ***refuse to sign* the authorization**
- **Disclosure of direct or indirect *remuneration* from a third party for use or disclosure of PHI**

Authorizations For Clinical Trials

Exception to general rules prohibiting:

- **Compound authorizations (§164.508(f)(2)): Authorization *may be combined* in same document as a:**
  - **consent to participate in research (informed consent form)**
  - **consent to use/disclose PHI for treatment, payment or health care operations**
  - **notice of privacy practices**
- **Conditioning of treatment on authorization: The provision of research-related treatment *may be* conditioned on provision of an authorization (§164.508(b)(4)).**

Authorizations For Research: Criteria for Waivers

§164.512(i)(2)(ii)

- **The use/disclosure of PHI involves *no more than minimal risk* to the individual**
- **The alteration or waiver *will not adversely affect the privacy rights and the welfare* of the individuals**
- **The research *could not practicably be conducted* without the alteration or waiver**
- **The research *could not practicably be* conducted without access to and use of PHI**
- **The privacy risks are *reasonable* relative to anticipated benefits, if any to the individuals, and the importance of the knowledge that may reasonably be expected to result from the research**

Authorizations For Research: Criteria for Waivers

- **Adequate plan to *protect the identifiers* from improper use and disclosure;**
- **Adequate plan to *destroy the identifiers* at the earliest opportunity consistent with conduct of the research, unless there is a health or research justification for retaining the identifiers, or such retention is otherwise required by law; AND**
- **Adequate written assurances that the PHI will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the research project, or for other research for which the use or disclosure of PHI would be permitted.**

IRB Approval of Authorization Waivers for Research

- **IRB must comply with federal regulations (*e.g.*, HIPAA) (§164.512(i)(1)(i)(A))**
- **IRB must apply the Common Rule *even to privately funded* research (§164.512(i)(2)(iv)(A))**
  - **IRBs must apply the Common Rule to privately funded research but *not* to privately funded clinical trials**

IRB Approval of Authorization Waivers for Research

- **What is "minimal risk" under the Common Rule?**
  - **The probability and magnitude of harm or discomfort anticipated in the research are not greater in and of themselves than those ordinarily encountered in daily life or during the performance of routine physical or psychological examinations or tests. (45 CFR 46.102(e))**
  - **Indexed risk: risk assessment must consider damage to financial standing, employability, insurability, reputation, or stigmatization**
  - **Genetic studies involving retrospective review of existing data and/or prospective blood draws pose *more than minimal risk* to subjects and are *not* eligible for waivers of informed consent. OHRP Guidebook for IRBs, Human Genetics Research, § 5-46.**

IRB Approval of Authorization Waivers for Research: Assessment of Minimal Risk

- **Exempt from IRB review (45 CFR 46.101(b)(4)):**
  - ***Existing* data, records, specimens, if**
    - **publicly available, or**
    - **unidentifiable**
- **Expedited IRB review (45 CFR 46.110)):**
  - ***No more than minimal risk*, and involves *only***
    - **Studies of existing data, records that have been collected *solely* for *non-research* purposes (*e.g.*, medical records)**
    - **Prospective collection of specimens by noninvasive means, or**
    - **Blood samples by venipuncture from healthy, nonpregnant adults**

Privacy Board Approval of Waivers For Research

Criteria

- Privacy boards are *not* required to apply the Common Rule
- HIPAA does *not* specify waiver criteria for privacy boards

Procedures (§164.512(i)(2))

- ≤ minimal privacy risk:
  - Board may use an expedited review procedure
  - Expedited review may be conducted by the chair of the privacy board or one or more board members designated by the chair
- > minimal privacy risk:
  - A *majority* of members must be present an dwaiver must be approved by a majority of those at convened meeting
  - ≥1 member unaffiliated with covered entity or sponsor

Documentation of Waiver Approval

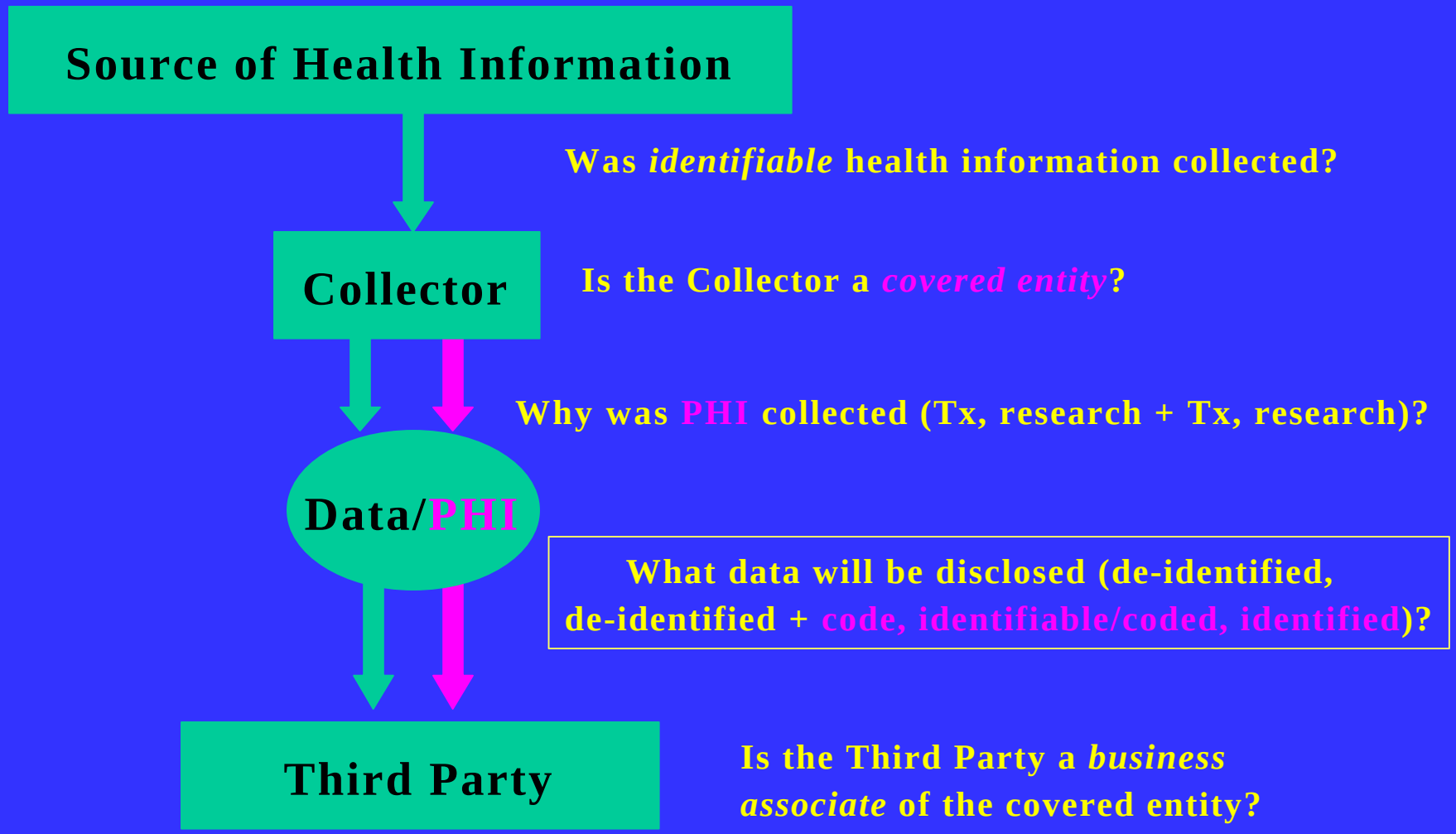
§164.512(i)(2)

- Identification of board and approval date
- Statement that waiver criteria were met
- Description of PHI
- Statement of whether normal or expedited review procedures were used
- Signed by the Chair (or designate) of the IRB or privacy board

PHI Collected For Research: Waiver Exception

- **Reviews preparatory to research (§ 164.512(i)(1)(ii))**
  - **Use/disclosure of PHI is solely to prepare a *research protocol* or for a similar purpose,**
  - **No PHI will be removed from the covered entity by the researcher, and**
  - **the PHI is necessary for research purposes**
- **Research on PHI from *decedents* (§ 164.512(i)(1)(iii))**
  - **Use/disclosure of PHI is solely for *research***
  - **Document death of individual**
  - **the PHI is necessary for research purposes**

Is Authorization Required?



What Information Will be Used/Disclosed?

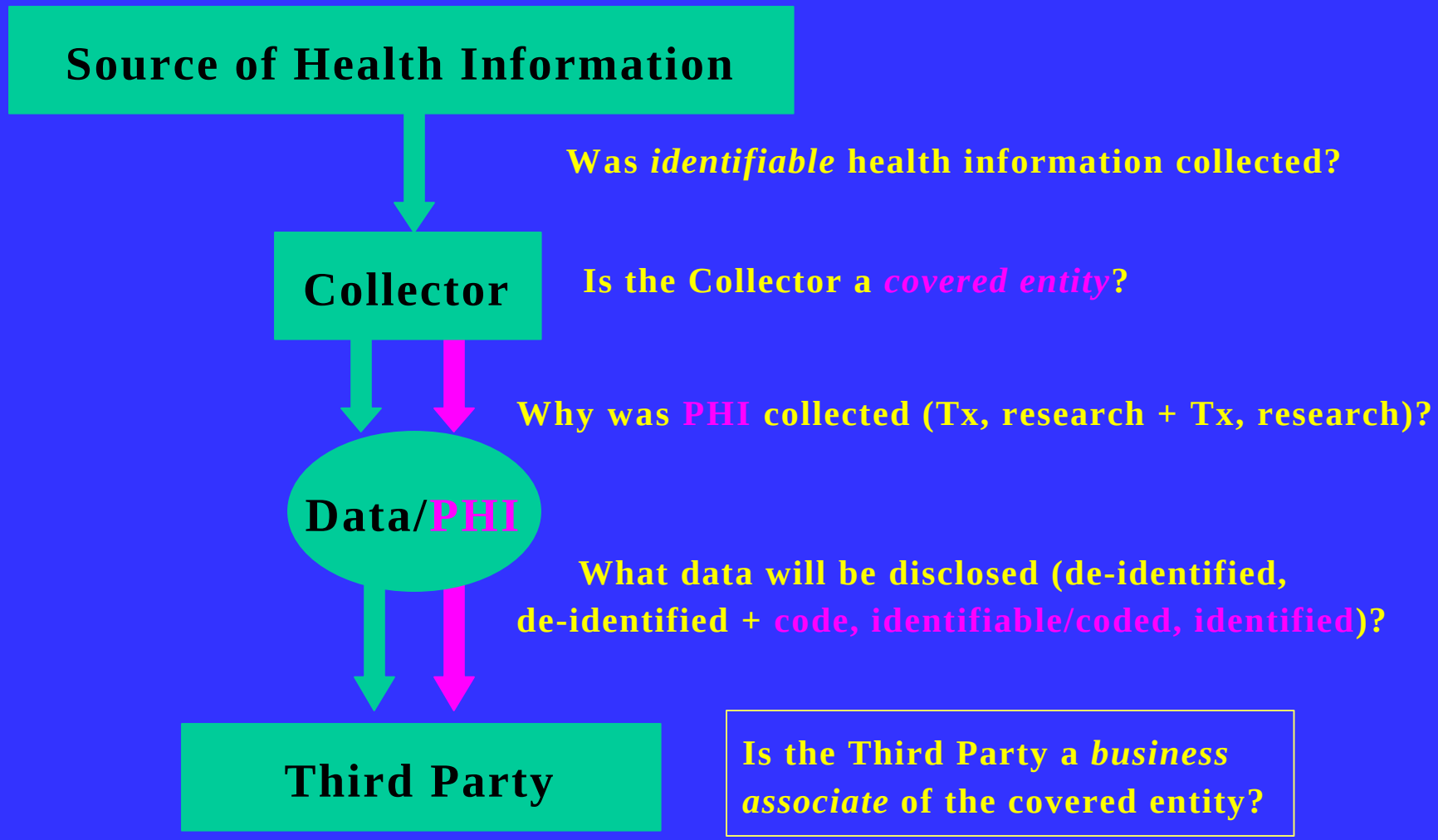
- Identified = PHI
- Identifiable (derived code) = PHI
- De-identified + derived code = PHI
- De-identified ≠ PHI

What Can be Disclosed?

HIPAA standard = Minimum Necessary

A covered entity must make *reasonable efforts* to limit PHI to the minimum necessary to accomplish the intended purpose of the use or disclosure.

Is Authorization Required?



Disclosure of PHI to Business Associates

§164.502(e)(1)

- Authorization is *not* required for:
  - A covered entity to disclose PHI to a BA
  - A BA to create or receive PHI *on behalf of* a covered entity
- <u>Providing</u> the covered entity obtains "satisfactory assurance that the BA will appropriately safeguard" the PHI
  - Assurance must be in writing
  - Business Associate Agreements (BAA) must meet requirements of §164.504(e)

Business Associates

- A person who is not part of the covered entity's workforce, who
- O*n behalf of* a covered entity
  - Performs functions or activities involving the use/disclosure of PHI, including:
  - data analysis, utilization review, quality assurance, claims processing
- *For* the covered entity performs a function that involves:
  - Disclosure of PHI from the entity to the BA, and
  - Legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services.
    - Data aggregation: Combining PHI from multiple CEs for *health care operations*, which do *not* include research.

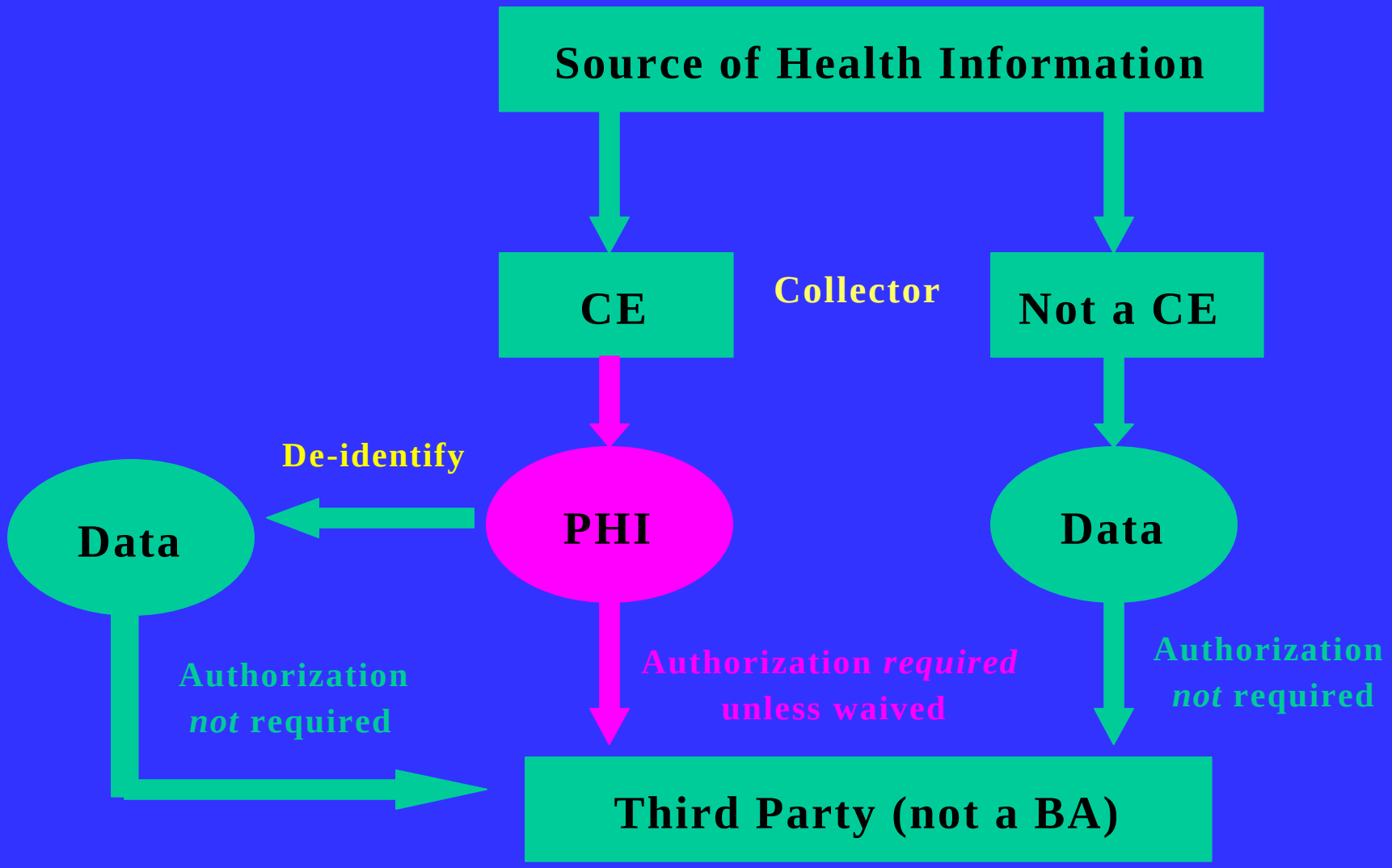
Business Associate Agreements

- The BAA must establish the permitted uses and disclosures of PHI by the business associate
- Business associates *may* use/disclose PHI:
  - As permitted by the BAA
  - Only as the covered entity could use/disclose the PHI
  - To de-identify PHI
  - As required by law

Who Is A Business Associate?

- **Private sponsors of research? No.**
  - **Sponsor is not performing a function *on behalf* of the covered entity.**
  - **Sponsor is not performing one of the 9 specified services *for* the covered entity**
- **Contract Research organization? Yes, if**
  - **CRO used a covered entity's PHI to perform data analysis *on behalf of* the entity**

Summary of HIPAA's Authorization Requirements



Not Done Yet -- What About State Laws?

- HIPAA preempts *only* state laws that are contrary to and less stringent than HIPAA
- Need to determine the floor of privacy protection in *each* state
- State medical confidentiality laws
  - General confidentiality of medical/health information
    - Research exceptions (variable)
  - Specific confidentiality laws (*e.g.*, *genetics*, HIV/AIDS, mental illness)
  - State health practitioner licensure laws

Hot HIPAA Research Issues

- Access to existing databases
  - Subject recruitment for clinical trials
  - Commercial data mining
  - DTC advertising
- Privacy board *vs.* IRB waivers of authorization for research
- Genetics research
  - Clinical trials or research (no feedback to subject)?
  - Authorization for research may be waived *only* IF *no more than minimal risk*
  - Merge existing clinical data with new genetic data
- Who is a "business associate"?
  - Private sponsors? Ph.D.s at AMCs? CROs?