HIPAA Privacy Regulations

Building Toward Group Health Plan and Issuer Compliance

presented at

The Second Annual HIPAA Summit

March 1, 2001

Mark E. Lutes, Esq.
Partner
Epstein Becker & Green, P.C.
1227 25th Street, N.W.
Washington, DC 20037
(202) 861-1824
mlutes@ebglaw.com

*The author wishes to thank his partners Ann Kaplan, Daly Temchine and Stephanie Kanwit for their helpful comments.

Building Block Definitions (I) §160.103

- **Group health plans:**

  Employee welfare benefit plan which either has 50 or more participants or is not administered by the sponsor.

- **Health insurance issuer:**

  Insurance company, HMO etc.

- **Health plan:**

  Group health plan, health insurance issuer, Medicare, Medicaid, Champus, FEHBP etc.

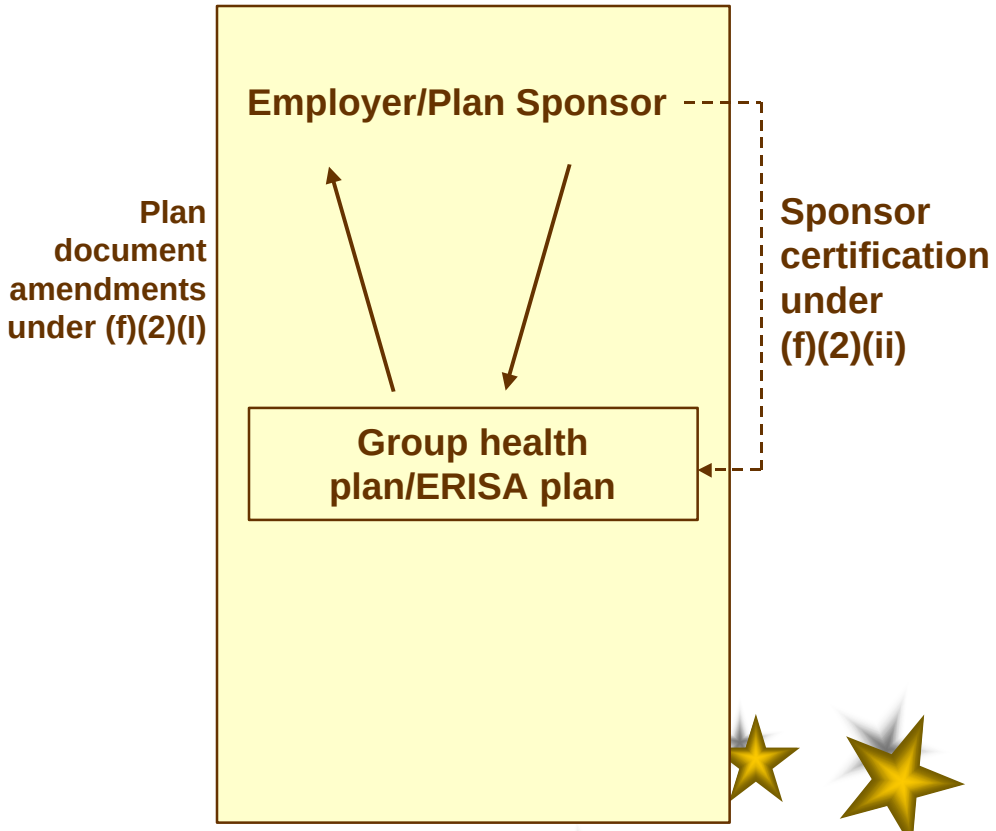
Building Block Definitions (II) §164.504

- **Hybrid entity:**
  - legal entity with covered functions that are not its primary function
- **Health care component:**
  - the parts of a covered entity that perform covered functions
  - a part that would be a business associate if the components were in two entities (e.g., performs a function and received PHI)

Relationship #1

MUSINGS

- Group health plan is a covered entity.
- Employer is not. Could it be the "business associate" of the Group Health Plan?
- Apparently it could be since the rule recognizes the sponsor and ERISA plan as separate legal entities. (Preamble at 82645)
- Also, the preamble notes that business associate contract would be required but for 504(f)(2) (Preamble 82508).
- Alternative approach "Hybrid entity"?



Requirements for Disclosure of PHI to Plan Sponsor/Employer

- **Always have a §508 authorization option … (but individual nature and disclosure details could be difficult)**
- **Special restrictions apply to "Big 3" (§ 506) disclosures - they are limited to summary health information unless the plan documents (in lieu of individual authorizations) establish what the sponsor can do with it and:**

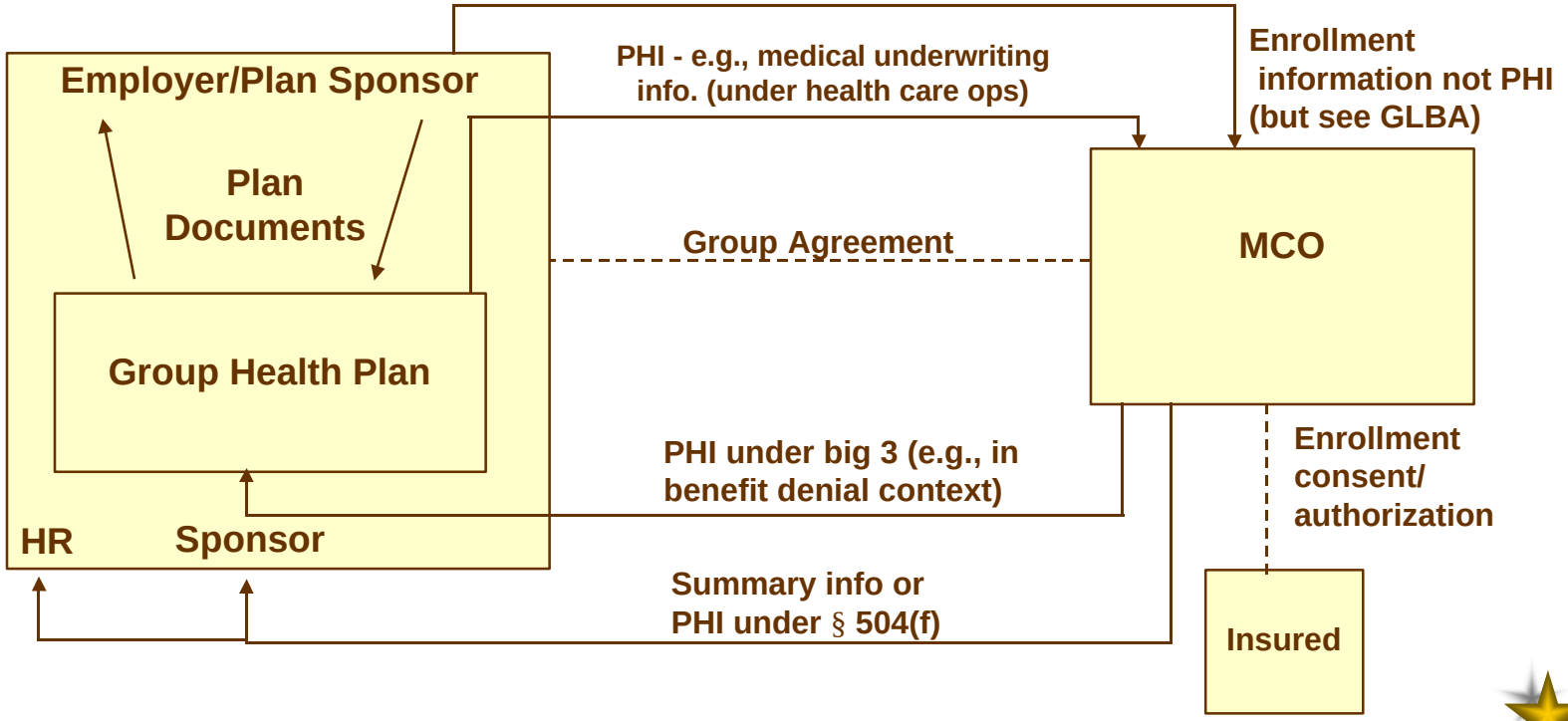
Requirements for Disclosure of PHI to Plan Sponsor/Employer (cont.)

- the uses are “consistent with the subpart” (catchall?)
- the sponsor makes a series of certifications to the group health plan e.g.,:
  - no use for employment-related actions
  - report breaches
  - available for amendment
  - return or destroy
  - access rules have been established

Implementation Requirements: §164.504(f)(3)

- **Seems to add a "plan administration" caveat to §(f)(1) and §(f)(2).**
- **Moreover, not only is group health plan required to amend plan documents and obtain sponsor certifications before GHP's own disclosures but:**
  - it must prevent a health insurance issuer from making such disclosures unless a specific statement has been included in its privacy policy and
  - even then, the sponsor cannot have an employment related purpose

Relationship #2



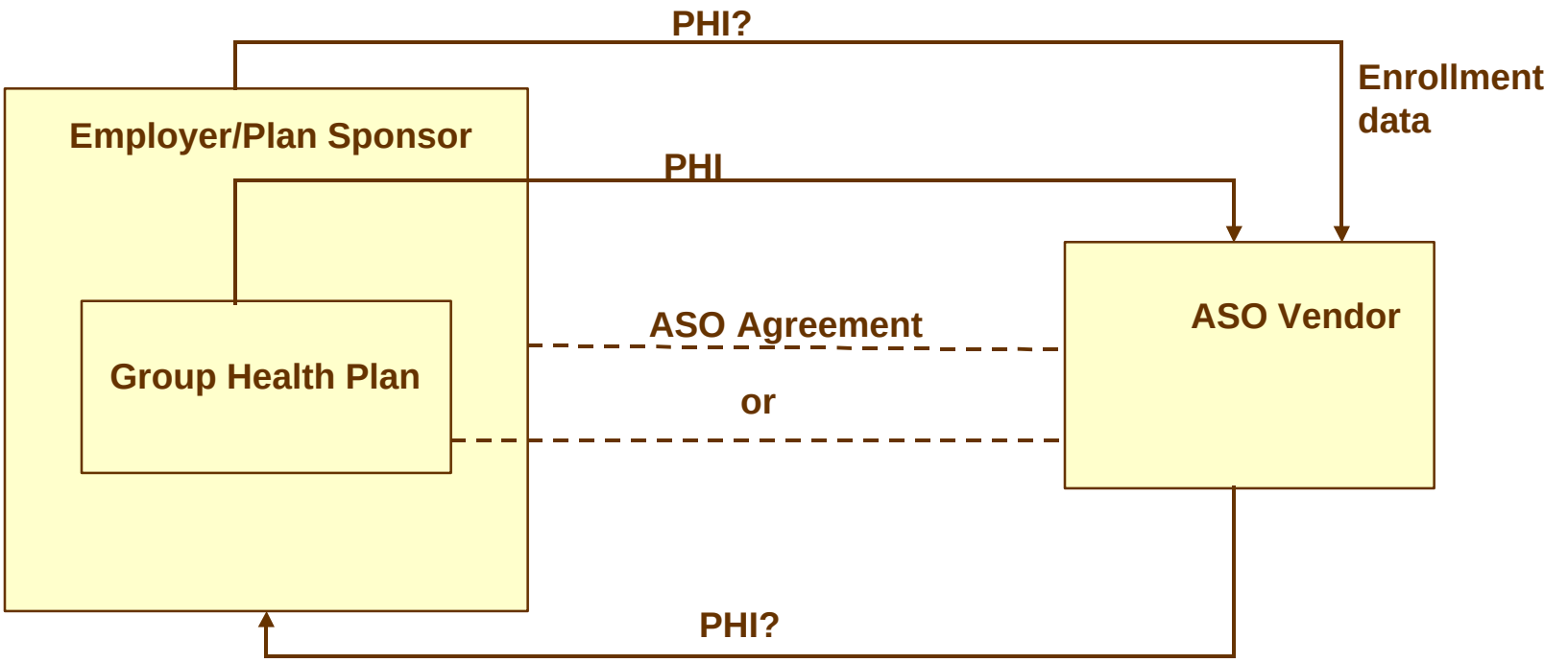
Relationship #2 (cont.)

- **Group Agreement Upgrades:**
  - **MCO gives GHP business associate covenants and the PHI information is identified? Preamble 82508 v. §160.103(ii).**
  - **MCO's Argument: "I am a covered entity anyway". GHP's Response: "Then why not give me the covenants?"**
  - **MCO gives GHP pledge not to disclose PHI except as permitted by 504(f)(2).**
  - **GHP certifies to MCO that Firewalls etc. are in place**
  - **Sponsor certifies to MCO that no employment use will be made and other 504(f)(2) covenants**

Relationship #2 (cont.)

- **What if employer needs PHI for fiduciary roles?**
  - plan documents
  - the MCO's privacy statement would need to address it
- **GHP makes decision to be in or out of PHI flow to avoid notice and administrative requirements? (Preamble 82509)**
- **What if EOC/COI serves as plan documents?**
- **Amend plan documents to reflect Big 3 disclosures to MCO and more if needed.**

Relationship #3



- ASO vendor not a covered entity in this context even if otherwise a covered entity.
- However, ASO vendor is business associate of GHP

Relationship #3 (cont.)

- **ASO agreement should contain business associate PHI identification and covenants probably even where ASO vendor contracts with sponsor**
- **ASO agreement should contain plan document upgrade covenants.**
- **Vendor's disclosures to sponsor not governed by §164.504(f). See 504(f)(iii). Therefore disclosures could be more extensive unless the ASO contract's business associate language limits them.**
- **What if the employer receiving the PHI is an MCO or hospital and thus a covered entity in its own right?**