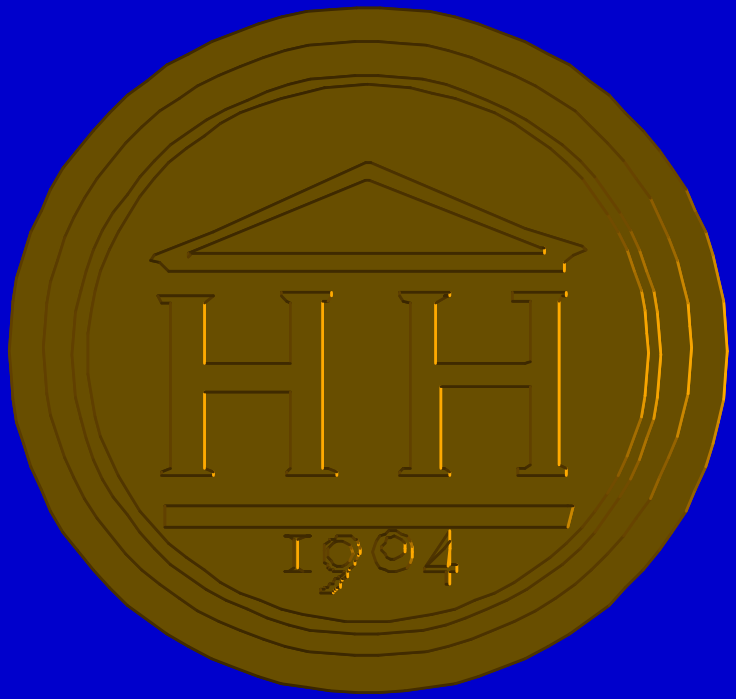

HOGAN & HARTSON, L.L.P.

http:\\www.hhlaw.com

"Publications"

"Health"

HIPAA: The Birth and Development of a Legal Identity Crisis

Donna A. Boswell

HOGAN & HARTSON, L.L.P.

The HIPAA Colloquium at Harvard University

August 22, 2002

HIPAA Speak:
Do you know the secret word?

- "PHI" -- protected health information
- "CE" -- covered entity
- "BA" -- business associate
- "OHCA" -- organized health care arrangement
- "P&P" -- policies and procedures

Speak friend and enter...

"A CE may not use or disclose PHI, except as permitted or required by [the HIPAA regulations -- privacy, transactions and code sets.]"

45 CFR 164.502(a)

NOTE: *If you are a CE, there is a HIPAA right way and a HIPAA wrong way to do everything involving PHI.*

Top Secret Hints for Lawyers:

- You only need *one* HIPAA right way to do a use or disclosure
  - Flexibility and scalability are HHS watchwords
- American law imposes obligations on "persons" -- living human beings, corporations, partnerships --

–BUT HIPAA DOES NOT.

Special Issues Affecting Providers' Compliance Burden and Obligations

HIPAA Legal Identity Crisis #1

"covered entity" "hybrid" entity

"health care component"

"business associate" "non-covered provider"

"OHCA" "workforce"

Perhaps the most critical implementation challenge for lawyers is establishing the relationships between these HIPAA structures and the legal entities and individuals that must implement the requirements.

HIPAA Structure: Hybrid Entity

- The corporation/partnership is not necessarily the covered entity
- The covered entity -- "health care component" is what you say it is.
- *But if* it includes the whole corporation-- the whole corporation's uses and disclosures, P&P, etc. must comply with the rule.
- May include *only* a component that performs a "covered function" or an "internal BA"

HIPAA Legal Identity Crisis #2

- When one of these HIPAA entities has a legal obligation--
  - Who -- what corporate or live person -- may perform it?
  - When does it "count" as compliance for a particular entity?
  - Who is liable if it is not performed?
  - How do you address "apparent agency" issues?

HIPAA Structures: OHCAs

1. Clinically integrated care setting (hospital)
2. Organized system of care --
   "Hold themselves out" as joint arrangement, *and* participate in joint activities (UR, QA, PMT)
3. Group plan and HII or HMO
4. 2 or more group plans of same sponsor
5. 2 or more group plans and HMOs, HIIs

HIPAA Structure: OHCA

- *May* have a joint notice; need *not* have the same P&Ps
- Need not have BAs for "joint activities" of the OHCA
- *May* include non-covered providers
- A living human being can be in an OHCA *and* be a separate covered entity (*or* non-covered provider)
- A covered entity can be in more than one OHCA

OHCA Issues

- Apparent agency liability?
- Liability for revocations of authorizations and exercise of certain rights (e.g., confidential communications, restrictions)
- Policies and procedures still required for physicians or must adopt hospital's
- Who will sign business associate agreement for OHCA?

HIPAA Legal Identity Crisis #3

- When a "use" is authorized, are there restrictions on *who* may do it?
- When a "disclosure" is authorized, are there restrictions on what the *recipient* may do with the information?
- Does the entity that is authorized to disclose have legal obligations *after* doing so?

Secrets of HIPAA Compliance: *Standards* for Uses and Disclosures 45 CFR 164.514

- De-identification (a) & (b)
  - Safe harbor vs. statistician certification
- Use of case codes (c)
- Minimum necessary (d)
- Limited data sets for research, public health, and health care operations (e)
- Fundraising (f)
- Underwriting (g)
- CE obligations regarding recipients (h)

HIPAA Structure: Business Associate

- "*On behalf of* such covered entity…performs or assists in the performance of:
  - "(A) A function or activity involving the use or disclosure of …[PHI], or
  - "(B) Any other function or activity regulated by this subchapter, or
- "…legal, actuarial, accounting, consulting , data aggregation, management, administrative, accreditation, or financial services… [involving PHI]

BA Issues? (P. 53253)

- A third party is not your BA PHI is for:
  - A covered function (e.g., treatment, payment), unless for the third party to perform the function on your behalf (e.g., billing)
  - A non-covered function, whether or not on your behalf, that is a disclosure permitted by the regulation (e.g., research, law enforcement, public health reporting)
  - An activity where PHI access is "incidental"

Why *not* do a BA -- just to be sure?

- If you have a BA agreement with a third party (whether required or not):
  - administrative cost of negotiating and keeping in place.
  - CE must cure, mitigate or report known violations
  - *for each patient request of an accounting, must have a mechanism to check BA's disclosures for purposes of providing the accounting.*

Secrets of HIPAA Compliance

What?	Having the piece of paper *w*ith the right *magic words*
Who?	In the right entity's hands
When?	Obtained at, and retained for, the right time
How?	Used to train, supervise, and hold accountable the right human beings.

Research is an Authorized Use/Disclosure

- "A CE may use *or* disclose PHI for research regardless of the source of funding for the research provided that--"
- The rule specifies the *three* entirely separate *alternative* mechanisms for meeting the HIPAA Who, What, When for research
  - Data Use Agreements 164.514
  - Authorization 164.508
  - Three distinct 164.512 mechanisms

Research With Authorization Is An Authorized Use/Disclosure

45 CFR 164.508

What: The Research Authorization must be signed by the patient, must include the "core elements;" may not violate "compound authorization" rules:

- may be combined with an informed consent for "the same research study"
- may have "none" as an expiration date
- may condition research participation on signing
- may limit termination rights

Who, When, How: CE has; before use or disclosure; retain 6 yrs from termination, last reliance, or expiration.

The 164.512(i) Research Mechanisms: Obtain any *one* prior to use or disclosure

- Waiver of authorization 164.512(i)(1)(i)
  - IRB/privacy board documents; CE has; retain 6 yrs from last reliance.
- Reviews preparatory to research 164.512(i)(2)(ii)
  - Researcher "represents"; CE has; retain 6 yrs. from last access
- Decedent's information 164.512(i)(
  - Researcher "represents"; CE has; retain 6 yrs. from last access

Research is an Authorized Use/Disclosure

- When the use *or* disclosure is with authorization
  - No BA; No accounting
- When the use is *by a HIPAA entity*--
  - NO BA Agreement
  - NO *disclosure* so accounting
- When disclosed to a third party in accord with the rule
  - NO BA Agreement, but accounting required
- What if a third party is doing research *for* the covered entity?

Data Use Agreement
45 CFR 164.514(e)

- Establish permitted uses (res., pub. health, HCO)
- Not further use or disclose
- Protect with safeguards from improper use
- Report impermissible uses and disclosures to CE
- Impose restrictions on agents and contractors
- Not identify or contact data subjects
- CE Issues:
  - Min. necessary -- may rely on representations
  - CE knows of non-compliance and fails to cure or report

Marketing
45 CFR 164.508

- Authorization required and must disclose remuneration
- Includes disclosure of PHI for direct or indirect $ for third party marketing.
- "To make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service, unless--
  - product or service of the CE; in the benefit plan
  - for treatment
  - for case management

HOGAN & HARTSON, L.L.P.

555 13th Street NW
Washington, DC 20004
202-637-5600
http:\\www.hhlaw.com