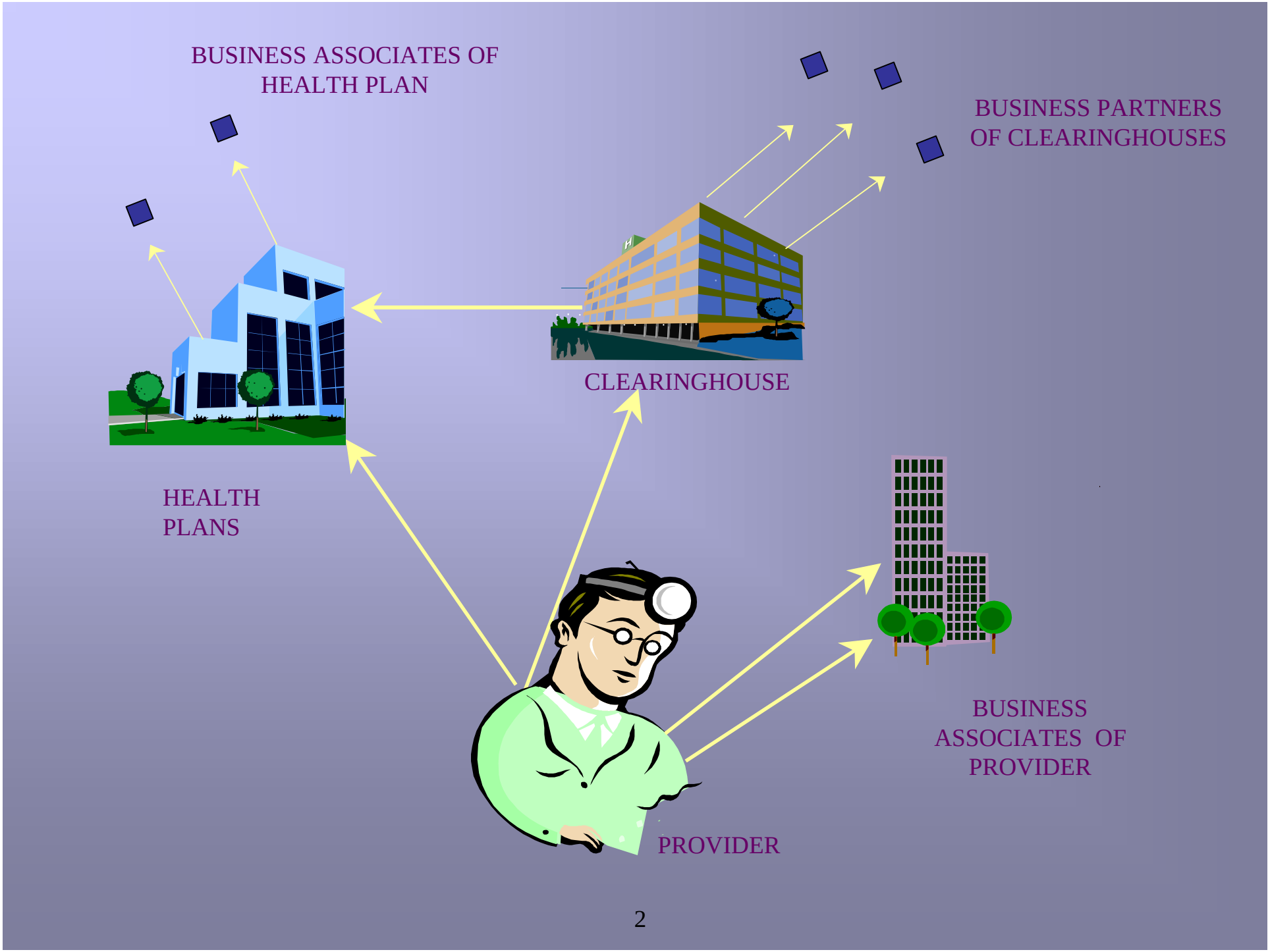
THE HIPAA SUMMIT WEST

June 21, 2001

BUSINESS ASSOCIATE AGREEMENTS UNDER HIPAA PRIVACY AND SECURITY RULES

Jackie Huchenski, Esq.
Moses & Singer LLP

.


BUSINESS ASSOCIATES OF HEALTH PLAN
BUSINESS PARTNERS OF CLEARINGHOUSES
CLEARINGHOUSE
HEALTH PLANS
BUSINESS ASSOCIATES OF PROVIDER
PROVIDER

PRIVACY RULE DEFINITIONS:

Covered Entities: Health plans, health care clearinghouses and health care providers who transmit any health information in electronic form in connection with a transaction covered by HIPAA or use a third party to do so on its behalf.

Business Associates: A person (i) who on behalf of the covered entity or organized health care arrangement perform[s], or assists in the performance of….. a function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management and repricing or any other function or activity regulated by this subchapter… or (ii) who [p]rovides… legal, actuarial, accreditation, consulting, data aggregation, management, administrative or financial services to or for such covered entity or organized health care arrangement….where the provision of service involves the disclosure of individually identifiable health information from such covered entity…to the person".

Nb: does not include members of workforce, members in same organized healthcare arrangement, or bank processing payments for CE

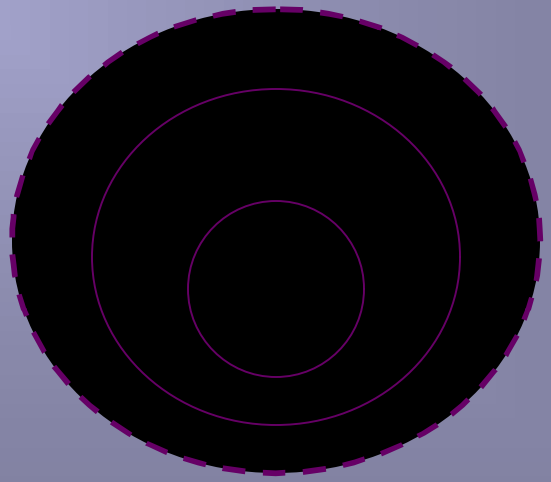
PROPOSED SECURITY RULE DEFINITIONS:

Covered Entities: similar to Privacy Rule.

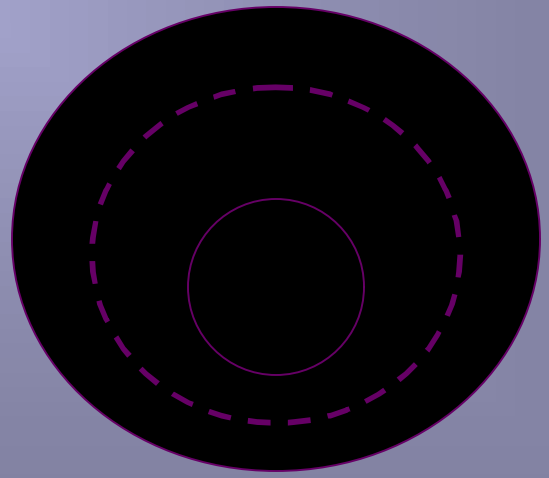
Business partner: not defined in the Security Rule, but the rule states that chain of trust agreements are required with "business partners" (preamble says "processors" of health information).

Note: "Business Associate" is defined in Part 160 which applies to all of Subpart E, including Security Rule.

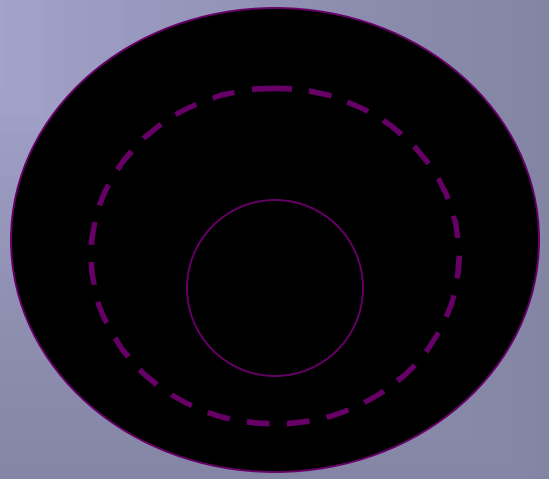
Health information: Any information, whether oral or recorded in any form or medium, that (1) is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse and (2) relates to the past, present or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual. [nb Security Rule covers “health information”]



"Individually Identifiable Health Information": Health information (including demographic information collected from an individual) created by or received by a health care provider, health plan employer, or health care clearinghouse (1) that identifies the individual or (2) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.



"Protected Health Information: Individually identifiable health information other than certain student records governed by FERPA.



BUSINESS ASSOCIATE AGREEMENT REQURED UNDER THE PRIVACY RULE:

A covered entity may not disclose protected health information to a business associate, and a business associate may not create or receive protected health information on covered entity's behalf, without a contract between the covered entity and the business associate to which information is to be disclosed that establishes the permitted and required uses and disclosures of such information by the business associate, except for:

(A) disclosures of protected health information by a covered entity to a health care provider for treatment purposes,

(B) disclosures by a health plan to a plan sponsor in certain cases, and

(C) disclosures under certain government programs where eligibility and administration are performed by two different agencies.

BUSINESS PARTNER AGREEMENT REQUIRED UNDER THE PROPOSED SECURITY RULE:

Covered entities must assess potential risks and vulnerabilities to the individual health data in its possession and develop, implement, and maintain appropriate security measures, which must be documented and kept current, *including chain of trust business partner agreements whereby the partners agree to electronically exchange data and protect the integrity and confidentiality of the data exchanged*. (emphasis added) [Note that "data" is used not "health information"].

What You Can Do Now:
Baseline Assessment

1. Identify third parties that receive protected health information or health information from your organization.

2. Determine number and status of any outstanding agreements with such third parties--will agreement expire before 4/13/03?

3. Review representative sampling of such agreements including terms of confidentiality provision or data transfer/ownership incorporated therein.

4. Compare Privacy Rule's 10 specific requirements for business associate agreements.

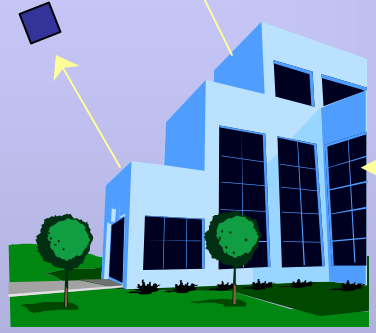
5. Review "amendment" and "invalid provision" terms to determine recommended approach (e.g. draft form of amendment for current agreements?)

6. Covered Entities have more leverage now (if cannot agree on BA agmt. with vendor, switching vendors may disrupt operations later).

7. State law may have BA agmt. requirements now (e.g. Connecticut -health plans).

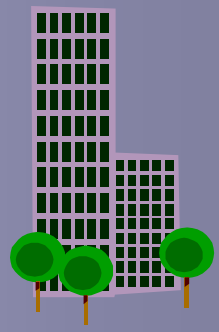
BUSINESS ASSOCIATES OF HEALTH PLANS

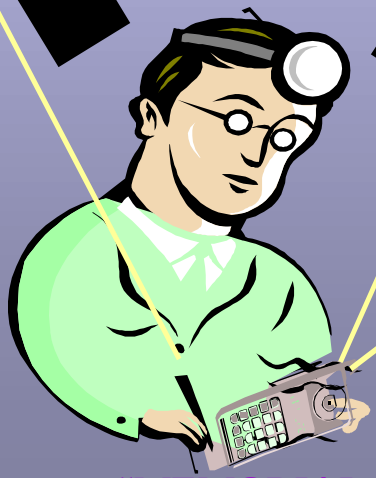
BUSINESS ASSOCIATES OF CLEARINGHOUSE



CLEARINGHOUSE

HEALTH PLANS





"MEMORIAL HOSPITAL"

"Scrip Checker"

- wireless services to determine adverse drug interactions to reduce medical errors

PRIVACY RULE

10 required terms in BA Agmt.

PROPOSED SECURITY RULE

2 required terms in COT Agmt.

Required Term 1:

Scrip Checker shall not use or disclose protected health information except as provided in this agreement or required by law. [permitted uses and disclosures must be defined further - limit according to BA's role, remember minimum necessary rule, state purposes for uses and disclosures and reasons for and types of persons to whom BA may make further disclosures]

- set parameters broadly or narrowly
- necessary to ensure that BA will be liable for breach (b/c BA not regulated directly)

Required Term 2:

Scrip Checker shall implement and maintain appropriate safeguards to prevent the use or disclosure of protected health information other than as provided herein.

- "appropriate" as determined by CE
- comparable to those maintained by CE, including administrative, technical and physician safeguards
- CE can require additional safeguards
- CE must approve of BA's measures

Required Term 3:

Scrip Checker shall report to *Memorial Hospital* any use or disclosure of protected health information in violation of this agreement or law of which *Scrip Checker* becomes aware.

- immediately
- ask for sanctions for employees
- CE must mitigate known harmful effects of violations
- additional safeguards

Required Term 4:

Scrip Checker shall ensure that any subcontractors or agents to whom it provides protected health information received from *Memorial Hospital (*or created or received by *Scrip Checker* on behalf of *Memorial Hospital)* agree to the same restrictions and conditions that apply to *Scrip Checker* with respect to such information.

- contain provisions similar to specific terms of this agreement
- right to review downstream contracts

Required Term 5:

Scrip Checker shall make protected health information available to the individual subjects of such information as required by *Memorial Hospital*.

- within specific timeframe
- in format required by CE
- to CE (not directly to individual)

Required Term 6:

Scrip Checker shall make its internal practices, books and records relating to the use and disclosure of protected health information received from *Memorial Hospital (*or created or received by *Scrip Checker* on behalf of *Memorial Hospital)* available to the Secretary of the Department of Health and Human Services for purposes of determining *Memorial Hospital's* compliance with HIPAA and with the Privacy Rule issued pursuant thereto.

- CE gets copy of information provided

Required Term 7:

At termination of this agreement *Scrip Checker* shall return or destroy all protected health information received from *Memorial Hospital (*or created or received by *Scrip Checker* on behalf of *Memorial Hospital)* that *Scrip Checker* still maintains in any form and retain no copies of such information. If such return or destruction is not feasible, *Scrip Checker* shall only use such information for purposes that make such return or destruction not feasible and the provisions of this agreement shall survive with respect to such information.

- within ____ days
- certify as to same
- CE to conduct audit
- de-identified information

Required Term 8:

Scrip Checker shall incorporate any amendments or corrections to protected health information when so notified by *Memorial Hospital*.

- timeframes provided in law, therefore within ___ days
- in format required by CE

Required Term 9:

Scrip Checker shall provide for an accounting of uses and disclosures of protected health information as requested by *Memorial Hospital.*

•No accounting required if disclosure was for treatment, payment or health care operations

Required Term 10:

Memorial Hospital may terminate this agreement if *Memorial Hospital* determines that *Scrip Checker* has violated a material term of this agreement.

- immediately upon notice
- specify "material terms"?
- CE must terminate if CE takes reasonable steps to cure breach and steps are not successful, unless termination is not "feasible", then report to Secretary of HHS

Optional Terms per Privacy Rule:

(1) *Scrip Checker* may (i) use protected health information for "proper management and administration", (ii) use protected health information to carry out legal responsibilities, or (iii) disclose protected health information if required by law or if *Scrip Checker* obtains reasonable assurances from recipient that recipient will keep information confidential and only use or further disclose if required by law or for purposes described in (i) or (ii) above.

(2) *Scrip Checker* may use protected health information for data aggregation services relating to *Memorial Hospital's* operations (i.e. combining PHI with PHI received from other covered entities to analyze health care operations).

Other Optional Terms:

- Indemnification
- Insurance
- Audit
- No third party beneficiaries unless required by law
- Business Associate will also have to comply with Covered Entity's notice of privacy policies and practices

Proposed Security Rule

Required Term A:

Scrip Checker shall provide, shall require its agents and subcontractors to provide, security for all data which is electronically exchanged between *Memorial Hospital* and *Scrip Checker*.

- as deemed “appropriate” by CE
- security checklist
- comparable measures
- right to review policies and to audit

Proposed Security Rule

Required Term B:

Scrip Checker shall implement and maintain, and shall require its agents and subcontractors to implement and maintain, appropriate and effective safeguards to protect the security and confidentiality of data electronically exchanged between *Memorial Hospital* and *Scrip Checker*, including access to data as provided herein.

Some Likely Additional Responses by BA:

1. Economics - who bears additional expense of complying with new agreement terms? BAs with leverage will negotiate.

2. Limit information provided to BA to "de-identified" information wherever possible.

3. Set standards (e.g. "reasonable" or "best efforts") wherever possible.

4. Negotiate terms not explicitly mandated by Rules (e.g. CE need not approve downstream contracts between BA and subcontractor)

5. Limit access to "BA's normal business hours upon reasonable notice" wherever possible.