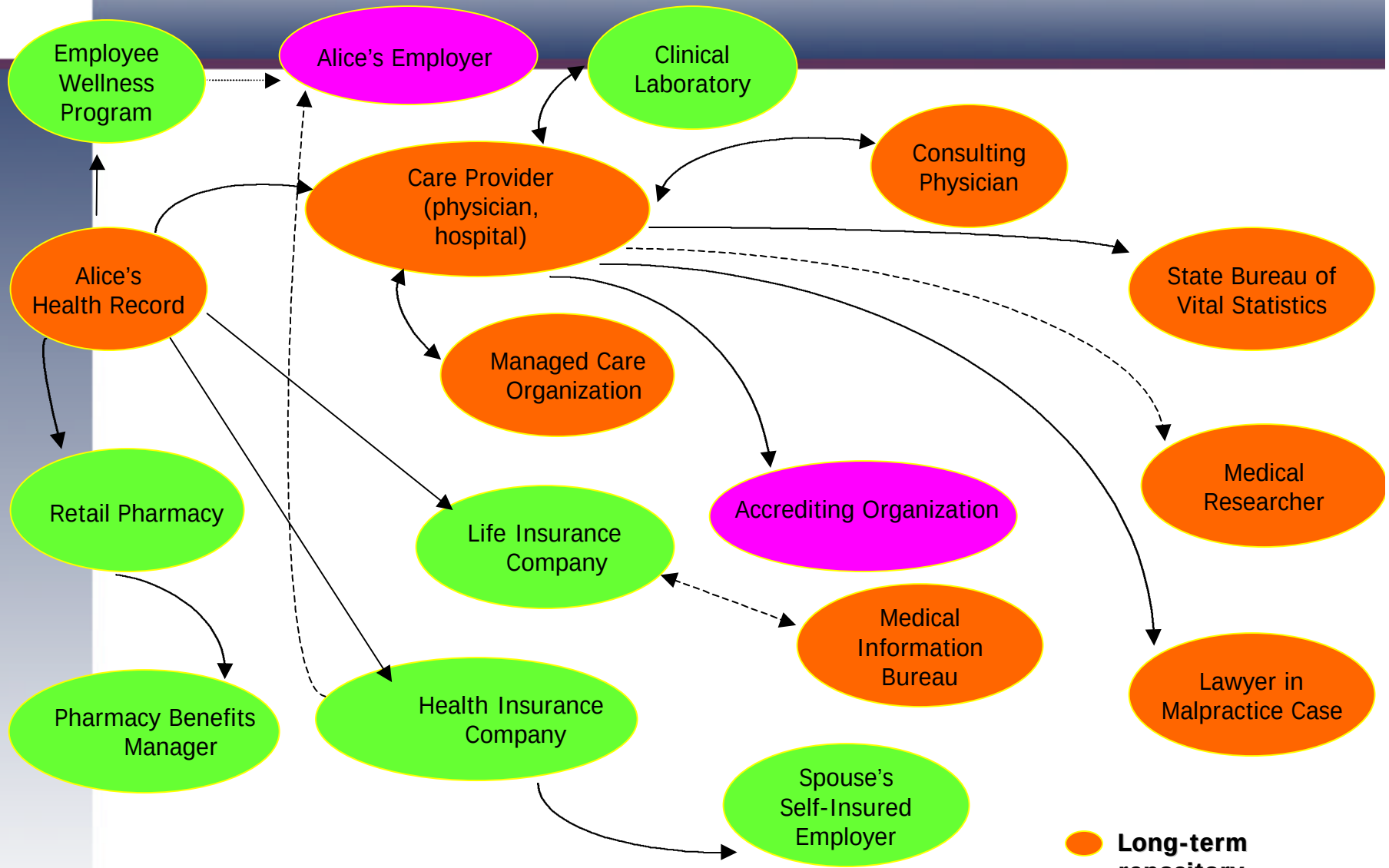
HIPAA Privacy Regulations: Access and Consent

Presented By: Michael L. Blau, Esq.
McDermott, Will & Emery
28 State Street
Boston, MA 02109
(617) 535-4010
mblau@mwe.com

The Flow of Medical Information



1191121-1

SOURCE: National Research Council, Computer Science and Telecommunications Board
For the Record: Protecting Electronic Health Information (Washington, DC: National Academy Press, 1997).

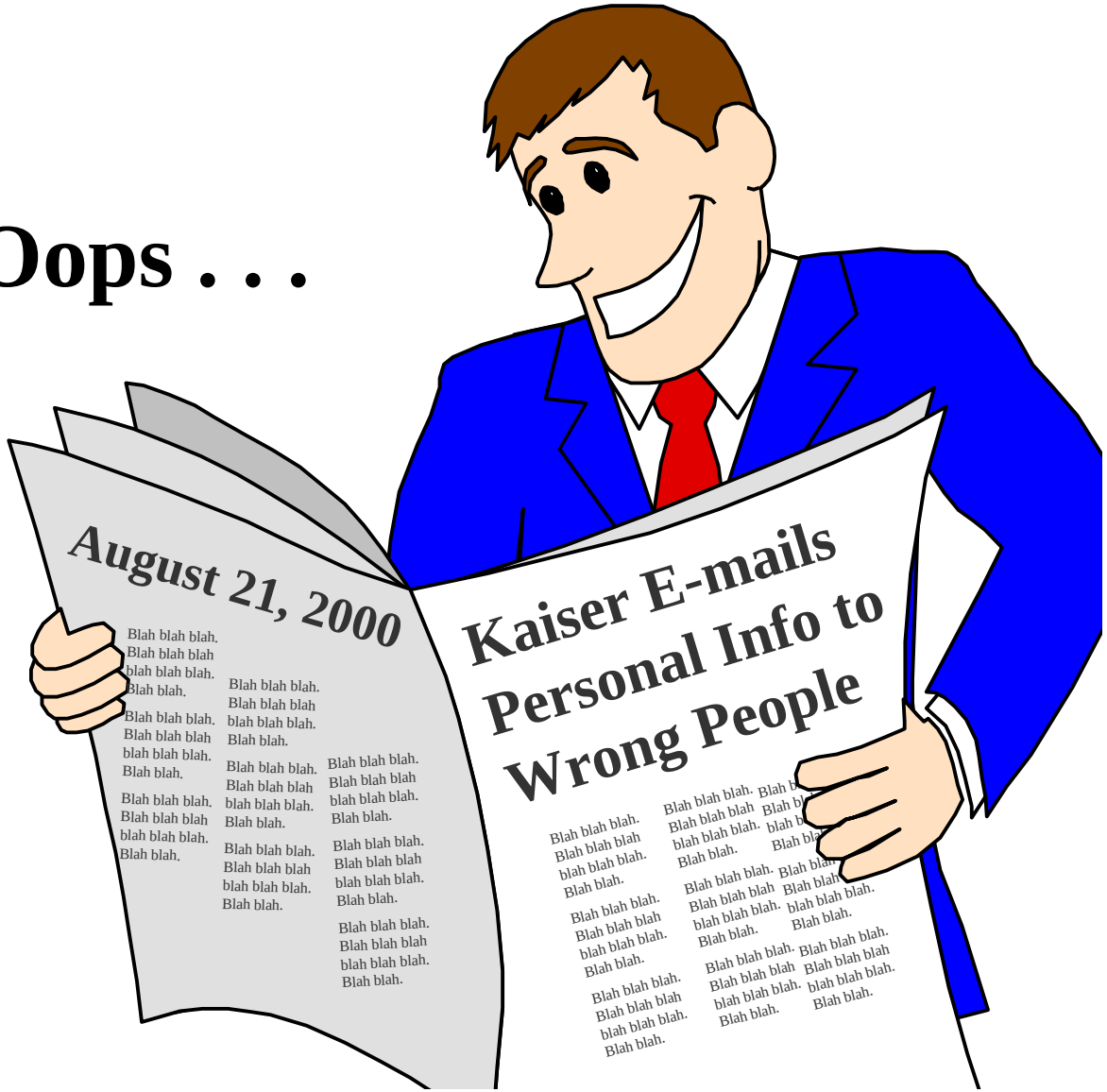
Privacy Concerns

- 75% concerned about information sharing without authorization
- 65% concerned about e-mail security
- 59% concerned about hacking
- 40% would not have their personal health record on-line; 38% would
- 37% feel that submitting any personal information is an invasion of privacy

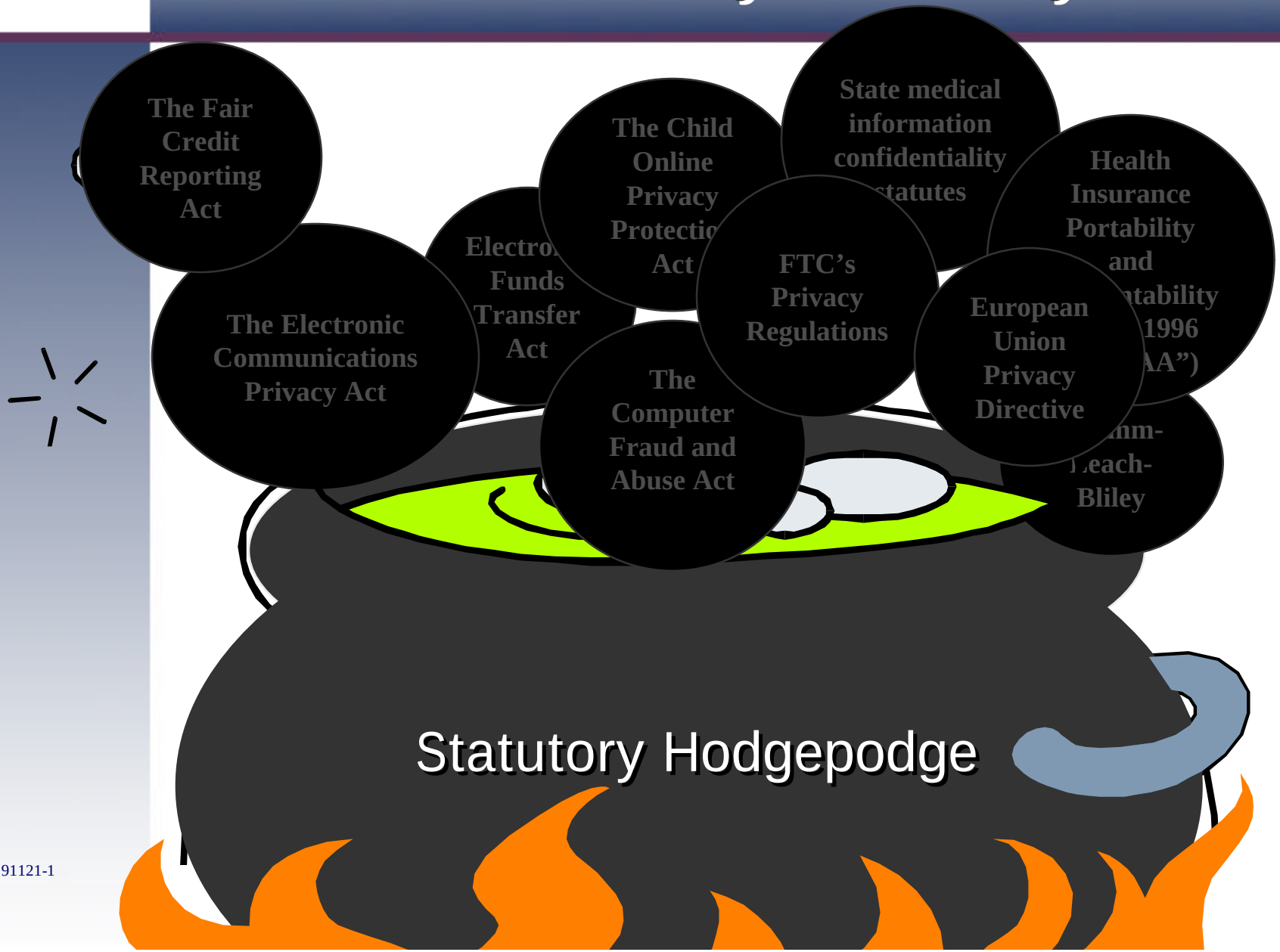
Cyber Dialogue, Deloitte Consulting (Feb., 2000)

Privacy/Security Concerns

Oops . . .



Privacy/Security



What is HIPAA?

Goal: Improve the efficiency and effectiveness of electronic information transfers used in the provision, management and financing of health care in the U.S.

- EDI Transactions and Code Sets (finalized)
- National Health Identifiers for individuals (on hold)
- Security Requirements for administrative, physical, and technical safeguards to assure data integrity, confidentiality and availability (proposed)
- Privacy Rules (finalized)

Permitted Uses and Disclosures of PHI

- With a proper Consent to carry out treatment, payment or healthcare operations
- Pursuant to a valid Authorization
- By opt-in/opt-out of the subject individual
- As required or permitted by law, e.g., investigations, emergencies

Consent Standards

- Form of consent and authorization governed by federal law
- Personal representative may count as individual
- Who is authorized to give consent and authorization governed by state law
  - capacity
    - minors/emancipated minors
  - competency
  - health care proxies
  - substituted judgment
  - implied consent

- Covered entity can disregard personal representative if it reasonably believes an abusive situation exists, or is not otherwise in individual's best interest.

General Rule for Patient Consents

(§164.506)

Consent must be obtained by Covered Health Care Providers for use of PHI for:

- Treatment
- Payment
- Health Care Operations: Q/A, credentialing, accreditation, peer review, protocol or formulary development, management, customer service, due diligence in connection with sale, compliance programs, case management, coordination of care, referrals to other facilities, training, arrangement of legal services and audits, business planning, population-based activities to improve health care or reduce costs, certain marketing and fund raising activities

General Rule for Patient Consents

(§164.506)

Consent Required Unless:

- Indirect treatment relationship (e.g., consultant physician)
- Emergency
- Required by law to treat
- Not possible to obtain consent due to substantial barriers to communication and consent inferred
- Inmates

General Rule for Patient Consents

(§164.506)

Consent Requirements:

- Must be in plain language
- Must inform individual re: use of information
- Must reference Notice of privacy practices
- Consent must not be combined with Notice, but:
  - may be combined with other permission forms if "visually and organizationally separate" and separately signed and dated, or
  - is part of a Research Authorization
- Must inform individual of right to request restrictions
- Must be signed and dated
- Must be revocable (except to extent of reliance)
- Not effective if any element is missing

General Rule for Patient Consents

(§164.506)

Other Consent Issues:

- May condition treatment on receipt of consent
  - More restrictive governs
- Joint Consents
  - Identify for organized health care arrangements covered entities to which consent applies
  - Satisfy general consent requirements
  - If consent is revoked, inform other covered entities of revocation

General Rule for Patient Authorizations

A Covered Entity may not use or disclose PHI for any reason (other than treatment, payment, health care operations) without a valid Authorization

- Generally applies to any use and/or disclosure not covered by a Consent, with limited exceptions
- Cannot condition treatment on receipt of Authorization
- Disclosure of psychotherapy notes (i.e., therapist's own notes of counseling session) requires Authorization for use in treatment, payment and health care operations; Consent will suffice:
  - for diagnostic or treatment summaries
  - for test results
  - prescriptions
  - for use in treatment by originator of notes
  - in training programs
  - to defend legal action
  - oversight of originator of notes

Requirements for Patient Authorizations

- Description of information in specific and meaningful fashion in plain language
- Name of person(s) authorized to make the requested use/disclosure
- Name of person(s) authorized to receive request
- Individual's right to revoke
- Information may be subject to redisclosure and not protected by the federal privacy regulations
- Right to inspect
- Right to refuse to authorize
- Disclose if direct or indirect remuneration to the Covered Entity will result
- Expiration date, signature, date, and copy

Marketing Communications

(§164.514(e))

- Authorization is not required (general consent will suffice) for:
  - Face to face discussions of products/services
  - Nominal value products/services
  - Beneficial health-related products/services of the Covered Entity or third party with disclosure of remuneration, why the individual was targeted, and how the product/service relates to individual's health
  - Allows individual to "opt-out" of receiving future communications (unless marketing occurs through general newsletter)
  - There is no disclosure to others except business associate assisting with the communication
- Special requirements for target marketing based on health condition

Fundraising Communications
(§164.514(f))

- Authorization is not required (general consent suffices) if:
  - Fundraising is for benefit of the Covered Entity only
  - Can disclose to related foundation that raises funds for Covered Entity
  - Only demographic information and date of care is used
  - Plans for fundraising communications must be referenced in general Notice of privacy practices
  - Allows individual to “opt-out” of receiving future communications

Authorizations and Consents

(§164.506)

- Resolving conflicts between consents and authorizations
  - more restrictive governs
  - obtain new consent that clarifies
  - communicate with individual and document expressed preference

Uses and Disclosures Requiring Opportunity for Individual to Agree or Object (§164.510)

- "Opt-in; Opt-out" orally or in writing - No consent or authorization required
  - opportunity to prohibit or restrict use
- Facility directories
  - name, location in facility, general condition, religious affiliation
  - Emergency exception
- Family members or others involved with the individual's care or treatment
  - If individual is present: inferences permitted
  - If individual is not present: professional judgment as to best interest of patient
  - Disaster relief

Permitted Uses and Disclosures By Regulatory Mandate (§164.512)

- Disclosure to the individual
- No consent, authorization, or opportunity to agree or object required
- Indirect treatment relationship for treatment, payment, health care operations
- Emergencies, where treatment is required by law, or where there are substantial communication barriers (not psychotherapy notes)
- Where required in HHS investigation or to determine compliance

Permitted Uses and Disclosures By Regulatory Mandate (§164.512) (cont'd)

- Required by law
- Public health activities
- Victims of abuse, neglect, domestic violence
- Health oversight activities
- Judicial and administrative proceedings attorney issued subpoenas
- Law enforcement purposes
- Decedents - funeral directors, coroners, and medical examiners
- Cadaveric organ, eye, tissue donation
- Research - waiver of authorization approved by IRB or a Privacy Board
- Serious threat to health or safety

Permitted Uses and Disclosures By Regulatory Mandate (§164.512)

(cont'd)

- Government functions - Armed Forces, national security, correctional institutions
- Workers' compensation
- Whistleblowers
- Workforce members who are crime victims

Minimum Information Necessary

- Covered Entity must reasonably ensure that it does not request, use or disclose more than the minimum amount of PHI necessary
  - May not disclose entire medical record, except to providers for treatment
  - Develop criteria to limit disclosures
  - Review requests for disclosures on an individual basis
  - For recurring requests, may develop standard protocols
  - Identify which members of work force require which items of PHI; limit access accordingly

Health Plans

- Although consents are required of health care providers for the use or disclosure of PHI for purposes of treatment, payment or health care operations, they are not required of health plans
- Key definition is “health care operations” in health plan context
- Reviewing the competence or qualifications of professionals, business planning and development, premium rating and other activities related to the creation, renewal or replacement of a contract of health insurance are examples
- Definition is broad enough to include case management and disease management activities

Health Plans: Required Authorizations

- Authorizations are required for purposes other than treatment, payment, or health care operations
- Health plans cannot condition enrollment or treatment on the individual's providing such an authorization except under the following circumstances:
  - The authorization sought is for the health plan's eligibility or enrollment determinations relating to the individual or for its underwriting or risk rating determinations prior to the individual's enrollment in the health plan
  - A health plan may condition payment of a claim for specified benefits on provision of an authorization if the disclosure is necessary to determine payment of such claim
- There are exceptions to both of the above when the use or disclosure of psychotherapy notes is at issue

Special Issues for Research

- The privacy standards for PHI will affect Covered Entities' research, and indirectly, affect pharmaceutical companies and medical device companies who sponsor research
- Three pathways for Covered Entities' disclosure of PHI to sponsors of research:
  - Pursuant to an Authorization (§ 164.508(f))
  - Pursuant to a Waiver of Authorization from an IRB or new Privacy Board (§ 164.512(i))
  - De-identification (§ 164.514(a))

Research Authorizations

- An authorization for use and disclosure of PHI must be obtained for research that includes treatment of individual subjects, including a description of the extent to which PHI will be used
  - Existing consents are grandfathered
- This pathway would apply to most prospective clinical research studies
- Authorization may be included with:
  - Consent to participate in research
  - Consent to use or disclose PHI for treatment, payment or health care operations
  - Notice of privacy practices

Exception for FDA Reports

- There is an exception to the authorization requirement for disclosure to pharmaceutical companies and medical device companies (as persons subject to the jurisdiction of the FDA) to:
  - report adverse events
  - enable product recalls
  - track products (as FDA-required)
  - conduct post-marketing surveillance (as FDA-required)

Research: Authorization Not Required When ...

- Under certain circumstances, disclosure of PHI for research is permitted without an authorization:
  - pursuant to a waiver from IRB or new Privacy Board
  - for review of PHI necessary to prepare a research protocol
  - the disclosure is sought solely for research on decedents
- The waiver pathway likely would be used for retrospective studies involving medical record reviews

Waiver of Authorization

- To grant a waiver, the IRB or Privacy Board must find that:
  - disclosure involves no more than minimal risk to the individual who is the subject of PHI
  - research could not practicably be conducted without PHI or waiver
  - privacy risks are reasonable in relation to anticipated benefits to the individuals and the importance of the knowledge that may reasonably be expected to result from the research
- To grant a waiver, the IRB or Privacy Board must find that:
  - there is an adequate plan to protect PHI from improper use and disclosure and to destroy identifiers at the earliest opportunity consistent with the conduct of the research
  - PHI will not be reused or disclosed to any other person (except as required by law or for authorized oversight of the research project)

Action Steps

- Implement by February 26, 2003 (2004 for small health plans)
- Review existing consent forms
- Remember that old consents are still good consents
- Evaluate whether joint consents should be used for multiple entities in system
- Develop new Consent form as part of (but visually separate from existing consents and separately signed and dated) or as separate document
- Develop Authorization form satisfying requirements (may be included with Consent form)
- Determine activities for which Authorizations will be needed on a recurring basis

Action Steps

- Forms should request and authorize use and disclosure only to minimum extent necessary
- Authorizations for research will also need to meet requirements for informed consents for clinical studies and be approved by IRBs
- Seek and document appropriate IRB waivers for research purposes
- Update privacy policy, and develop and post notice of privacy policy
- Include opt-in/opt-out right in marketing and fundraising materials
- Seek verbal/written agreement for inclusion in facility directories and disclosures to family/friends and clergy
- Document exercise of opt-in/opt-out rights
- Document situations of inferred consent; who has authority to infer consent?

Action Steps

- Document evidence of authority of personal representatives
- Configure document flow for medical records maintenance
- Develop process for implementing revocation of consents/ authorizations and restrictions on use
- Maintain psychotherapy notes separate from other medical records of individual
- Comply with more stringent state law requirements
- Develop educational materials and train staff regarding consent/authorization requirement

Forms are no good without people who know how and when to use them