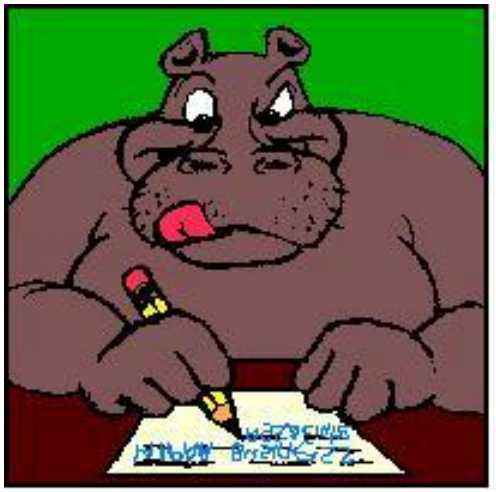
Dealing with Business Associates

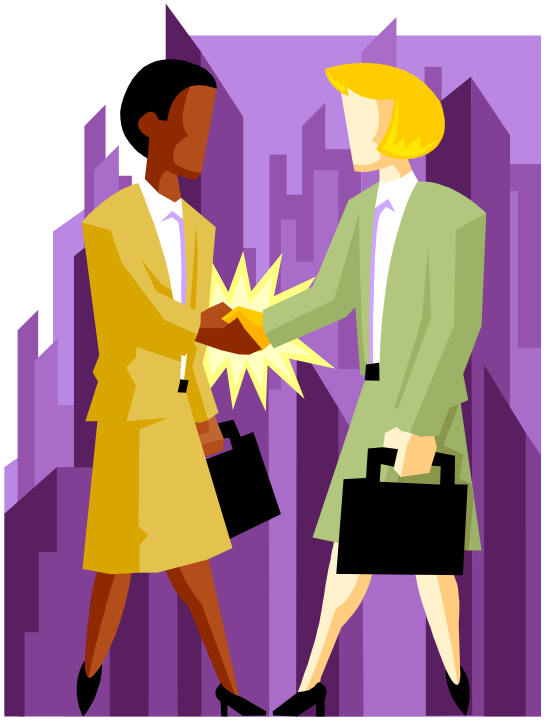


Business Associates

- Business Associates are persons or organizations that on behalf of a covered entity:
  - Perform any function or activity covered by HIPAA
  - Provide a service on behalf of a covered entity involving the transfer of PHI

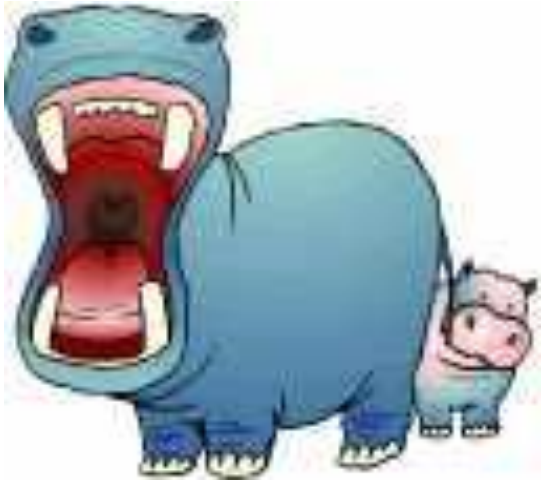
Some DHS Business Associates include:

- Medi-Cal Managed Care Plans
- Electronic Data Systems (EDS)
- Delta Dental
- Ramsell
- Maximus



HIPAA & Managed Care Plans

Medi-Cal Managed Care plans are covered entity health plans under HIPAA



Under federal law the state Medicaid agency must ensure that:

Each plan has written policies regarding enrollee rights including:

- Right to request and receive a copy of their medical records and
- Right to request that records be amended or corrected

42 C.F.R. §438.224

State Medicaid Agency must ensure:

- That plans use and disclose individually identifiable health information in accordance with privacy requirements in the HIPAA Privacy Rule

What Does This Mean?

1. Review plan policies and procedures to make sure HIPAA Privacy policies are in place

2. Monitor plan compliance with Exhibit “G” of the managed care contracts.

What Does Exhibit “G” Require?

- Plans may only use and disclose PHI for purposes directly connected to Medi-Cal administration
- Plans must provide DHCS contract manager with a list of external entities, except for network providers, to which it discloses lists of Medi-Cal member names and addresses (annually)

What Does Exhibit “G” Require?

- Not to divulge Medi-Cal status except for TPO
- To implement administrative, physical and technical safeguards
- To maintain comprehensive written information privacy and security program

Notification of Breach

Under Exhibit “G”, plan is required to:

1. Notify DHCS contract manager within **24 hours** during a work week of any suspected or actual breach of security or unauthorized use or disclosure of PHI
1. Take prompt corrective action and investigate the breach

Notification of Breach

3. Comply with state breach law found at California Civil Code §1798.82 and notify patients of unauthorized disclosure of personal information which is computerized and unencrypted
4. Provide a written report to DHCS Privacy Officer within 15 days of the discovery of the breach

NPP's

Under Exhibit "G" plans are required to:

- Produce a NPP which must include the DHCS Privacy Officer contact information for use by beneficiaries wanting to complain
- Submit new or revised NPP's to DHCS contract managers for review

New Revised BA Agreement

- DHCS negotiations with Maximus
- Strengthens the following areas:
  - Compliance with the Security Rule
  - Notification of breaches
- Two versions
  - High Risk – for FI's (including EDS and Maximus)
  - Standard Risk
- Revised 12/2007
- Managed Care plans
  - Use Exhibit G

THE END