Advanced HIPAA Issues for Biotech and Life Sciences Companies:

On the Frontier of Science and On the Edge of HIPAA

Mark E. Schreiber
Palmer & Dodge LLP
111 Huntington Avenue
Boston, MA 02199
617-239-0585
mschreiber@palmerdodge.com

April 8, 2005
HIPAA Provisions under which Biotech / Life Sciences Issues Arise

- HIPAA provider coverage?
- Business Associate applicability?
- Authorizations – unspecified research
- Research data bases
- Accounting for research disclosures
- Clinical studies in E.U. – HIPAA interface
**Medical Device / Testing Companies – Covered Entities?**

- May be “health care provider” under broad HIPAA definition
- Most don’t engage in electronic standard transactions
- Some may unwittingly send claims, insurance or related e-mails
- If so, possible HIPAA coverage
- Not all ask right questions of right people
  - To properly determine status

**If covered, then what?**

- Privacy notices, etc.
- To whom?
Are Clinical Researchers / Sponsors or CRO’s Business Associates?

Generally “research” not a BA function performed for covered entities

“We’re not a BA” letter

BA’s often negotiated
  Business clout

If researcher / sponsor also provides
  Quality assurance, or
  Data processing services for covered entity
    De-identifying records, or
    Creating limited data sets
  Then researcher / sponsor is BA

Researcher / sponsor – document in CTA that no BA-triggering services provided
Sponsors Generally Not Covered Entity or BA

No HIPAA concerns, then, right? *Not so fast* . . .

Sites will and should impose handling restrictions in CTA’s

Some sites impose informed consent confidentiality limitations

  Blending with HIPAA standards, on researchers / sponsors and “downstream”

  Restricts marketing use
Sponsors Generally Not Covered Entity or BA

Confidentiality agreement OK, but modify agreements

To specifically allow

For monitoring services, and

Other purposes in HIPAA-compliant patient authorization

Other agreement “pass-throughs”

Reps and warrantees, indemnity language

Researchers / sponsors – rigorous privacy policies / practices that approximate those of HIPAA

HIPAA treated as de facto standard of care

State law invasion of privacy claims
## Authorizations – Future Unspecified Research

HIPAA authorizations for research

- Can broadly cover patient’s entire medical record
- Can broadly cover classes or persons to whom and by whom PHI can be used / disclosed

Under “purpose” element,

- “Each purpose” must be specified

Valid authorization for **unspecified** studies

- Virtually impossible under HIPAA
- Registry or database for unspecified future research – OK
Research Databases under HIPAA

Database – separate purpose from primary protocol
Must be specifically authorized
   In protocol authorization or
   In separate subsequent authorization
If database maintained by covered entity
   Future disclosures must be pursuant to new authorization
If database disclosed to sponsor
   Generally outside HIPAA
IRB Waivers and Future Researcher Follow Up with Participants

If IRB Waiver

Researcher free to use PHI for current research

New, specific waiver necessary

Before researcher can contact study participants about new study
Accounting for Research Disclosures

**NEED NOT** be accounted for where
- Disclosed under authorization
- Disclosed in limited data set form
  - Needs data use agreement

**MUST** be accounted for upon individual request where disclosed pursuant to IRB waiver

Less detailed accounting:
- Where covered entity discloses records of 50 individuals under IRB waiver during requested accounting period
### Coming HIPAA Attractions: Clinical Studies Abroad and Outsourcing

<table>
<thead>
<tr>
<th>E.U. Model different – no HIPAA statute but broader data laws</th>
</tr>
</thead>
<tbody>
<tr>
<td>E.U. Data Protection laws</td>
</tr>
<tr>
<td>Each E.U. country</td>
</tr>
<tr>
<td>Consent necessary for medical data use (sensitive data)</td>
</tr>
<tr>
<td>Specific use, purpose, etc.</td>
</tr>
<tr>
<td>English or in local language?</td>
</tr>
<tr>
<td>Data transfer out of E.U. country to U.S.</td>
</tr>
<tr>
<td>Consent to transfer – different from consent to use / collect</td>
</tr>
<tr>
<td>Data protection model clauses / agreements</td>
</tr>
<tr>
<td>U.S. Safe Harbor</td>
</tr>
<tr>
<td>Who Follows Up on E.U. Branch Office or E.U. Consents?</td>
</tr>
<tr>
<td>------------------------------------------------------</td>
</tr>
<tr>
<td>Some companies not aware of or abide by these laws</td>
</tr>
<tr>
<td>Risk to studies?</td>
</tr>
<tr>
<td>Sometimes requires explanation of importance</td>
</tr>
<tr>
<td>E.U. clinical directive</td>
</tr>
</tbody>
</table>

**Is foreign medical PHI subject to HIPAA when transferred to U.S. HIPAA covered entity?**

- Telemedicine
- Medical records of E.U. resident sent to U.S.
<table>
<thead>
<tr>
<th>Outsourcing of HIPAA Data Processing Overseas</th>
</tr>
</thead>
<tbody>
<tr>
<td>Canada, India, Pakistan, Philippines</td>
</tr>
<tr>
<td>Medical transcription services</td>
</tr>
<tr>
<td>Pakistan case – multiple contractors to HIPAA covered entity</td>
</tr>
<tr>
<td>Rep. Markey letter to HHS</td>
</tr>
<tr>
<td>Possible outsourcing amendments to HIPAA</td>
</tr>
</tbody>
</table>