GW&T

OFFSHORE OUTSOURCING IN HEALTH CARE: PRIVACY AND SECURITY CONCERNS

CONCURRENT SESSION IV

September 9, 2005

Gregg D. Reisman, Esq.
Peter B. Mancino, Esq.
On behalf of
Garfunkel, Wild & Travis, P.C.

GW&T

WHAT IS OFFSHORE OUTSOURCING?

Offshore Outsourcing is the transfer or delegation of a business process to an external service provider located outside of the United States.

GW&T

BUSINESS PROCESSES COMMONLY PERFORMED OFFSHORE

- Transcription
- Data entry for medical billing
- Interpretation of radiology images
- Coding
- Claims review and adjudication
- Nurse call centers
- Information technology services

GW&T

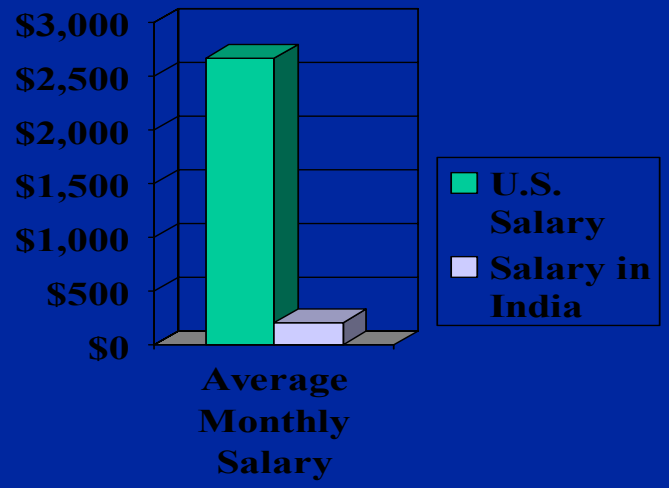
WHY ARE HEALTH CARE ENTITIES INCREASINGLY SENDING WORK OFFSHORE?

- Lower labor costs
- Shortages of allied health workers in the United States
- Ability to utilize time zone differences - e.g., the middle of the night in Chicago is the middle of the day in Bangalore, India
- Need for specialized training
- Desire to concentrate on core competencies
- Better results

GW&T

EXAMPLE OF LOWER OFFSHORE COSTS: AVERAGE SALARIES FOR TRANSCRIPTIONISTS

- Average annual salaries in the U.S. for transcriptionists have been flat since 1999, ranging from $27,000 to $32,000.
- Average transcriptionists in India earn the equivalent of $150-$200 a month or $1800-$2400 a year.



GW&T

WHAT CAN GO WRONG WITH OUTSOURCING?

- CitiGroup lost personal data for 3.9 million customers (UPS lost computer tapes).
- Time Warner lost data on 600,000 employees (backup tape lost in shipping by an outside data-storage company).

GW&T

WHAT CAN GO WRONG WITH OUTSOURCING? (cont'd)

- The case of the Pakistani Medical Transcriptionist:
  - In 2003, the University of California at San Francisco Medical Center received a threatening email from a Pakistani transcriptionist.

GW&T

WHAT CAN GO WRONG WITH OUTSOURCING? (cont'd)

- The Hospital had contracted for transcription services from an American company, and unbeknownst to the Hospital, some of its work was subcontracted out to Pakistan.

GW&T

WHAT CAN GO WRONG WITH OUTSOURCING? (cont'd)

- The transcriptionist claimed that she had not been paid and threatened to release patient information on the Web.
- This threat was retracted when the transcriptionist received payment. A breach was averted.

GW&T

GENERAL CONCERNS WITH THE USE OF OFFSHORE ENTITIES

- Licensure and Qualification Issues.
- Multiple Privacy Concerns: International Laws and Enforcement of U.S. Privacy Laws.
- Difficulty in enforcing contracts.
- Loss of jobs/effect on economy.
- Human rights issues.

GW&T

STATE LAWS GOVERNING OUTSOURCING

- Colorado – Proposed bill prohibiting the transmission of individually identifiable health information outside the U.S. without the consent of the individual. (Senate Bill 05-060)
- California – Recent enactment of a law governing the release of medical information. (West's Ann. Cal. Civ. Code § 1798.81.5)

GW&T

COLORADO

- The proposed bill would require a health care business (e.g., health insurer, health care facility, or health care provider) to notify an individual that his/her individually identifiable health information may be transmitted outside the U.S.
- Written consent of the individual must be obtained prior to transmission.
- Consent must be obtained annually and an individual could revoke consent at any time.
- Prohibits discrimination if an individual refuses to consent.
- 2/10/05 – Colorado Senate Committee on Health and Human Services postponed the Bill indefinitely.

GW&T

CALIFORNIA

- Effective January 1, 2005 – “Security Procedures and Practices With Respect to Personal Information About California Residents.”
- “A business that discloses personal information (defined to include individually identifiable medical information and other data) about a California resident pursuant to a contract with a nonaffiliated third party shall require by contract that the third party implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification or disclosure.”

GW&T

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996

- HIPAA requires that a “Covered Entity” have appropriate administrative, technical and physical safeguards in place to protect the privacy of protected health information.
- Covered Entities must contractually obligate business associates to protect health information through Business Associate Agreements.

GW&T

APPLICABLE BUSINESS ASSOCIATE AGREEMENT *PRIVACY REQUIRMENTS*

- A BA Agreement specifies how a BA may use and disclose PHI generally.
- A BA must agree to use appropriate safeguards to prevent the use or disclosure of PHI other than as permitted by the BA Agreement or as required by law.
- The BA must ensure that its agents and subcontractors who receive PHI agree to the same conditions and restrictions.

GW&T

APPLICABLE BUSINESS ASSOCIATE AGREEMENT *PRIVACY REQUIRMENTS* (cont'd)

- The BA must report to the Covered Entity any use or disclosure of PHI not provided for by the BA Agreement of which the BA becomes aware.
- The BA Agreement must allow for termination for a material breach.

GW&T

APPLICABLE BUSINESS ASSOCIATE AGREEMENT *SECURITY REQUIREMENTS*

- BA's must agree to implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of electronic PHI.

GW&T

APPLICABLE BUSINESS ASSOCIATE AGREEMENT *SECURITY REQUIREMENTS* (cont'd)

- BA's must ensure that their agents and subcontractors who receive PHI agree to implement reasonable and appropriate safeguards.

GW&T

APPLICABLE BUSINESS ASSOCIATE AGREEMENT *SECURITY REQUIREMENTS* (cont'd)

- BA's must report security violations.
- The BA Agreement must allow for termination for a material breach.

GW&T

COMMENTS

1. HIPAA does not apply to business associates or their agents directly.
2. A Covered Entity is not responsible under HIPAA for the acts of business associates or their agents, unless the Covered Entity knew of a pattern of activity or practice that constituted a material breach or violation and failed to take reasonable steps to cure or end the breach or violation.
3. Enforcement of HIPAA standards with respect to a business associate falls on the Covered Entity.

GW&T

PENDING LEGISLATION AIMED AT OFFSHORE OUTSOURCING

- Safeguarding Americans from Exporting Identification Data Act (SAFE-ID)
- Personal Data Offshoring Act of 2004

GW&T

SAFE-ID ACT

This Act proposes to prohibit business enterprises from disclosing personal identification information regarding U.S. residents to any branch, affiliate, subcontractor, or unaffiliated third party located in a foreign country unless certain criteria have been met.

GW&T

PRIOR TO DISCLOSURE, A BUSINESS ENTITY MUST:

- Provide a notice of privacy protections and comply with specific federal laws (e.g., Gramm-Leach-Bliley or HIPAA).
- Offer the consumer the opportunity to object prior to any disclosure.
- Notify the consumer about how to exercise his/her non-disclosure option.

GW&T

HOW WOULD SAFE-ID AFFECT HIPAA?

- All entities that send health information offshore would be required to revise their Notice of Privacy Protections.

GW&T

AMENDMENTS TO NOTICE OF PRIVACY PROTECTIONS

- Language would be added notifying the patient that PHI is being sent offshore.
- A description of the privacy laws in the offshore country would be provided to patients.
- Risks and consequences of shipping such work offshore must be listed.

GW&T

AMENDMENTS TO NOTICE OF PRIVACY PROTECTIONS (cont'd)

- The notice must describe the additional measures the entity will take to protect the privacy of PHI.
- Notification must be given that PHI will not be sent offshore if patient objects.
- A certification by the Covered Entity.

GW&T

CERTIFICATION BY COVERED ENTITY MUST:

- State that the Covered Entity has taken reasonable steps to identify the locations where PHI is outsourced.
- Attest to the privacy and security of PHI outsourced for processing offshore.
- State the reason for the determination by the Covered Entity that the privacy and security of such information is maintained.

GW&T

COVERED ENTITIES WOULD BE PROHIBITED FROM:

- Terminating existing relationships with consumers to avoid objections to disclosure; and
- Discriminating against qualified consumers of health care services due to such objections.

GW&T

HOW WOULD THE ENACTMENT OF SAFE-ID AFFECT HIPAA COVERED ENTITIES?

- Covered Entities may be forced to contract with multiple entities for the performance of the same service.
- Dividing up patients based on who consents/who does not consent could be a logistical nightmare.
- Potential civil liabilities for Covered Entities for sending a non-consenting patient's PHI offshore.

GW&T

PERSONAL DATA OFFSHORING PROTECTION ACT OF 2004

- This Act seeks to prohibit the transfer of personal information (including medical records) to any person outside the U.S. unless the person is notified and provides consent.
- This Act would provide a private right of action for recovery of actual monetary loss.

GW&T

CURRENT STATUS OF PENDING LEGISLATION

- SAFE-ID: Introduced and referred to the Committee on the Judiciary by Senator Clinton on April 14, 2005.
- Personal Data Offshoring Protection Act of 2004: Introduced on May 14, 2004 and has been inactive since.

GW&T

SO YOU STILL WANT TO OUTSOURCE OFFSHORE?

- Choices:
  - Utilize a domestic Vendor with an offshore capability or
  - Go directly to an offshore Vendor.

GW&T

THREE STAGES OF IMPLEMENTATION

1. Pre-Migration
2. Migration
3. Post-Migration

GW&T

PRE-MIGRATION

- Develop an RFP / Term Sheet
- Perform due diligence
- Negotiate & Finalize Outsourcing Contract
- Train personnel that will interface with the Vendor

GW&T

RFP / TERM SHEET

- Develop an RFP/Term Sheet that:
  - Sets forth specific business needs, requirements and contract terms.
  - Requires potential Vendors to explain how they will address your needs and requirements.

GW&T

CONDUCT DUE DILIGENCE

- Ask QUESTIONS!
- Review the laws of the offshore country.
- Review the policies and procedures of the offshore entity.
- Check references.

GW&T

DUE DILIGENCE *QUESTIONS*

- Where are the services being performed?
- Does the Vendor subcontract out work or send data to other locations?
- Vendor's financial stability?
- Prior security or privacy breaches?

GW&T

MORE QUESTIONS

- Does Vendor have a HIPAA compliance program and reasonable privacy and security policies & procedures?
  - Does Vendor provide HIPAA training?
  - Are background checks performed on employees?
  - Are employees required to enter into confidentiality agreements?
  - Are documents shredded?

GW&T

MORE QUESTIONS (cont'd)

- Does the Vendor comply with all HIPAA technical requirements?
  - Do employees have individual passwords and user accounts?
  - Does the Vendor's system have auditing capabilities?
  - Does the Vendor utilize encryption?

GW&T

MORE QUESTIONS (cont'd)

- Is equipment scrubbed prior to its disposal?
- Are network databases properly segmented so one client organization cannot access the data of another?
- How are documents physically secured?

GW&T

REVIEW THE LAWS OF THE COUNTRY WHERE THE SERVICES WILL BE PERFORMED

- Determine whether the country where the work is to be performed has adequate privacy protections.
- Consult appropriate legal counsel.

GW&T

CONTRACTUAL PROVISIONS

- Data Control:
  - Prohibit the Vendor from subcontracting without the Covered Entity's permission.
  - Prohibit the Vendor (and any subcontractors) from sending any health information outside of the United States unless the Covered Entity specifically agree.

GW&T

CONTRACTUAL PROVISIONS (cont'd)

- Expressly state that the Covered Entity maintains continued ownership and control of data.
- Require that the Vendor make all workers sign confidentiality agreements.
- Restrict assignment of the agreement.
- Permit the Covered Entity to conduct periodic audits.

GW&T

CONTRACTUAL PROVISIONS (cont'd)

- Require the Vendor to comply with applicable U.S., state and local laws and regulations including privacy standards:
  - For offshore vendors - consider listing the more significant laws/regulations in an appendix to the Agreement.
  - Expressly require compliance with HIPAA and a Business Associate Agreement.
  - Expressly state that United States Federal law and applicable state laws will control.
  - Specify that the United States is the proper venue.

GW&T

CONTRACTUAL PROVISIONS (cont'd)

- Require the offshore entity to provide training to its employees.
- Provide for security checks on employees prior to hiring.
- Require the Vendor to maintain security and privacy standards at least equal to those of the Covered Entity.
- Describe the implementation of required internal and external security safeguards that are appropriately updated.

GW&T

MORE CONTRACTUAL PROVISIONS (cont'd):

- Add provisions which:
  - Require the Vendor to provide prompt notice of a privacy or security breach or loss of personal data.
  - Include required steps that the Vendor must take in case of a breach.

GW&T

CONTRACTUAL PROVISIONS (cont'd)

- Include additional provisions which:
  - Grant the Covered Entity liquidated damages in the event of a breach of security/confidentiality/privacy.
  - Provide for indemnification.
  - Include bonding requirements.

GW&T

TRANSITION SERVICES

- Contracts should include transition services requiring:
  - The cooperation with a new Vendor.
  - The Vendors provision of data in electronic format that can be transferred to and utilized by new Vendor.
  - A transition period long enough to allow the Covered Entity to obtain an alternate Vendor.

GW&T

MIGRATION

- Perform simulations
- Consider utilizing a pilot program
- Require the Vendor to maintain backups/alternate site locations:
  - If possible, in the United States.
- If possible, limit the amount of data in the Vendor's possession.
- Require a business continuation plan.
- Develop disaster recovery/business continuity/crisis management procedures.

GW&T

POST MIGRATION
MONITORING THE VENDOR

- Ensure that privacy and data security controls are maintained throughout relationship.
  - Personnel security
  - Network security
  - Information security
- Monitor continued adherence with contractual terms and laws, regulations, rules, and best practices.

GW&T

INSURANCE CONSIDERATIONS

- Require that Vendors have adequate insurance.
- Will the Covered Entity's insurance cover acts or omissions by foreign vendors?

GW&T

IN THE EVENT OF A SECURITY/PRIVACY BREACH…

GW&T

MITIGATE DAMAGES
BE PREPARED!

- Public Relations.
- Reporting Obligations - comply with all applicable laws.
- Consider notifying the patient.
- Prepare for potential sanctions under HIPAA.
- Consider alternate vendors.

GW&T

QUESTIONS

Gregg D. Reisman, Esq.
Garfunkel, Wild & Travis, P.C.
111 Great Neck Road
Great Neck, New York 11021
greisman@gwtlaw.com
(516) 393-2294

Peter B. Mancino, Esq.
Garfunkel, Wild & Travis, P.C.
111 Great Neck Road
Great Neck, New York 11021
pmancino@gwtlaw.com
(516) 393-2286

GW&T

SOURCES

- SLIDE #5: "*Physician Paperwork Swept Offshore,*" by Tyler Chin, Amnews (May 10, 2004).
- SLIDE #6: "*Outside Firm Loses Time Warner Employee Data,*" Reuters (May 2, 2005).
- SLIDE #6: "*Info on 3.9M Citigroup Customers Lost*," CNN Money (June 6, 2005).
- SLIDE #7-9: "*A Tough Lesson on Medical Privacy: Pakistani Transcriber Threatens UCSF Over Back Pay,*" by David Lazarus, San Francisco Chronicle (October 22, 2003).