Alliance Alert

The Public Employee Benefits Alliance (PEBA) was created by a group of Texas Government leaders working together for over a year to develop strategies to manage the rising costs of healthcare benefits. PEBA was established in January 2006 and was created pursuant to Chapter 791 of the Texas Government Code, the Purchasing Program Chapter 271 of the Texas Local Government Code and all other applicable provisions of Texas Law. PEBA membership is open to all Texas local governments who pay an annual membership fee and execute a PEBA Participating Interlocal Agreement. However, local governments who are members of one of the political subdivision Pools will obtain automatic annual PEBA membership through the participating Pool. An additional per proposal fee is established for proposal participants for all non-Pool members.

PEBA's mission is to support the individual members by providing: negotiation services to manage the spiraling cost of healthcare and related benefits, working together through the alliance procurement model to purchase healthcare and related benefits at a competitive price, and provide contractual negotiations which will include vendor service accountability requirements. In order to accomplish this mission, PEBA makes a commitment to negotiate on behalf of the membership affordable, high-quality healthcare and related benefits and services.

PEBA met to review proposals that were submitted for the PEBA HIPAA Security Protected Health Information Audit. The Board made the decision to extend the Spohn Consulting with the agreement for an additional three years. During the interview and negotiation process, PEBA was guaranteed that Spohn has the capability to audit Healthcare Plan covered entities, Provider covered entities such as employer emergency services and employer on-site health clinics or virtual clinics.

Prior to the PEBA Board recommendation, the PEBA staff reviewed the CMS security rules to ensure compliance would be achieved. Below are the CMS common security rules that should be achieved during the covered entity audit.CMS cites common security rule issues that include:

1. **Risk Assessment:** Covered entities do not perform a risk assessment, lacked a formal documented risk assessment process or had risk assessments that were outdated or did not address all potential areas of risk. CMS called for risk assessments of "all systems and applications which store, process or transmit e-PHI" to be conducted" at least every three years or whenever there is a significant change in the environment.
2. **Currency of Policies and Procedures:** Covered entities were slow to review security policies and procedures or failed to document this process. The procedures documented were not always the ones actually followed.
3. **Security Awareness and Training:** Covered entities did not have formally documented training policies, did not track and retain evidence of training completion, granted user access before training completion or failed to refresh the training regularly.
4. **Workforce Clearance:** Covered entities granted access to e-PHI before completing background investigations.
5. **Workstation Security:** Covered entities lacked a formal documented process for verifying the security of workstations, were not complying with their policies and procedures for securing workstations or did not deploy the necessary tools to implement documented policies.
6. **Encryption:** Was not implemented on all workstations and laptops or on the transmission of data containing e-PHI, or strong encryption was not consistently implemented.

Component	Small	Medium	Large
Number of Sites	1	1	2
Total Number of Servers	4	65	110
Number of External Facing Servers	2	8	12
Number of External Facing Addresses	16	32	1024
Number of Network Domains	1	2	2
Number of Wiring Closets	1	15	40
Total Number of Firewalls and IDS	1	2	5
Number of Routers	1	15	35
Number of Switches	2	30	80
Number of Workstations	30	600	1500
Pricing	**$14,332**	**$37,516**	**$62,981**
***PEBA Pricing – Sample**	**$11,466**	**$30,013**	**$50,385**

Compliance and Regulation(HIPAA, HITECH, TMPL)

Regulations and recommendations from federal and state government as well as industry groups place additional security requirements on business and growing responsibility on business leaders for compliance. Many regulations offer only vague recommendations for security controls subject to interpretation and subsequent implementation by the business. Some provide specific requirements that must be addressed, documented and maintained. At the heart of all these compliance efforts is an attempt to establishment a minimal set of standard security controls that ensure the confidentiality, integrity and availability of certain respective protected information and the systems and networks wherein they reside.

The expansion of HIPAA regarding the HITECH Act details five items that must be included in breach notices. The HITECH Act details will be included in the audit. In addition to HIPAA/HITECH, the new Texas Medical Privacy Law puts far more stringent regulations in place for entities handling ePHI – Electronic Protected Health Information and expands the scope of "covered entities" beyond HIPAA or the HITECH Act. The Spohn Consulting HIPAA Security Audit addresses these regulations and provides organizations direction in avoiding these penalties by accomplishing compliance.

Under Texas HB300 – covered entities include: those engaged in the practice of assembling, collecting, analyzing, storing or transmitting ePHI or PHI; those that come into the possession of ePHI or PHI; those that obtain or store ePHI or PHI or is an employee, agent, or contractor of a person described above – if maintaining, using, transmitting, receiving, obtaining, or creating PHI or ePHI. IAW Texas Health and Safety Code, §181.001(b)(2).

The Texas Medical Privacy Law contains much stiffer civil and criminal penalties – enforced by the Texas Attorney General. Depending on the level of intent – stealing vs accidental disclosure – displayed in committing any particular violation; penalties can be anywhere from 1,500 dollars to 1.5 million dollars for every year of PHI or ePHI disclosure. These penalties or fines are above and beyond any levied by the federal government under HIPAA or HITECH, additional punitive actions can include revocation of licensing.

Alliance Alert

PEBA would like to invite you and your staff to participate in a Webcast to discuss the PEBA / Spohn Consulting Alliance and the offerings available to the PEBA membership:

WEBCAST INFORMATION:

When: Thursday, August 23, 2012

Time: 10:00 am CT

Registration: To register for this Webcast at no cost, contact PEBA at peba@tmliebp.org or at (512) 719-6768. We will need your name and title, email address and employer/group name to reserve a space.

Spohn Consulting's overview of services includes:

- Vulnerability Audit
- Firewall Audit
- Audit Virus Scanner
- Business Continuity Plan Review
- Review PHI and Security Policy and Procedures
- Operational Interviews for Procedure Compliance
- Physical Infrastructure
- Software Architecture
- Network Topology
- Identification of Potential Threats
- Determine Potential Threats and Exposure to Threats
- Compile Exit Report
- Remediation Recommendations
- Security Awareness Training

If you are interested in accessing the PEBA HIPAA Security Protected Health Information Audit service the employer will be requested to provide the following information to obtain employer pricing.:

Number of sites visited _____
Primary site city _____
Secondary site city (if applicable) _____
Number of employees _____
Number of external hosts _____
Number of public IP addresses _____
Number of file & print servers _____
Number of database servers _____
Number of web servers _____
Number of application servers _____
Number of other servers _____
Number of domains _____
Number of workstations _____
Number of wiring closets _____
Number of switches _____

Number of routers _____

Number of firewalls & IDS _____

All Pricing is custom and a completed pricing form is required in order to receive a detailed statement of work specific to your environment.

For political subdivisions that have not joined PEBA and/or did not participate in this proposal process, it is not too late. Political subdivision employers may still access the PEBA Alliance contracts if they are current with the PEBA Annual Membership Fee, Proposal Cost, Late Fee (if appropriate) and Interlocal Agreement. PEBA has demonstrated proposal success due the PEBA membership cooperation and support.

For more information, please contact PEBA directly: (800) 348-2879 ext. 6768.