Action Plan for Providers and Suppliers: Breach of Protected Health Information

The Philadelphia Inquirer recently reported that Keystone Mercy Health Plan and AmeriHealth Mercy Health Plan, two regional and sizeable insurance companies, lost a portable computer drive containing sensitive client information at a community health fair. Neither insurance company is apologizing for having brought their members' unencrypted health information to the fair. "By having this information readily available, we are able to save lives," said Donna Burtanger, vice president of communications for the firms.

Apparently company officials realized on September 20, 2010 that a portable drive containing the records of 285,691 Medicaid clients was missing. When the companies announced the security breach, a statement said the records were on a "flash drive for use at community health fairs." Burtanger also disclosed "That flash drive was never intended to leave the building."

The two insurance companies service 400,000 eastern Pennsylvania members on medical assistance. The insurers, she said, had been working to improve a method for allowing encrypted patient information to be available to company representatives at local health events. The drive was being used at headquarters to test the new system, she said. However, the information on the missing portable drive was not encrypted. It was also reported that the two companies had embarked on an initiative to encrypt all company data, including data on devices such as laptops or flash drives that would be used outside the building.

The September 20 incident occurred before the initiative was completed. The insurance companies would set up a booth at a community fair and when a member of the insurance carrier stopped by the booth, a representative of the insurance companies would check to see what the member's health history was; e.g.; when the member's last mammogram was, and then schedule an appointment for a mammogram.

The representative was not sure where the flash drive was: lost, thrown away or possibly stolen. The majority of the missing records, 285,691, containing health-plan identification numbers and results of recent screenings, did not contain member names. A total of 2,203 records did contain names with varying combinations of addresses, member identification numbers, and telephone numbers. Names and all or part of Social Security numbers are included on 808 records. The representative said that free credit monitoring would be provided to those whose Social Security numbers were involved and that letters to members would be sent out announcing a toll-free number for assistance.

HIPAA And HITECH

What Constitutes A Breach Of PHI?

The Health Insurance Portability and Accountability Act (HIPAA) and the recently enacted Health Information Technology for Economic and Clinical Health Act (HITECH) govern protected health information (PHI) privacy and security provisions. In summary, Covered Entities, such as the above mentioned insurance companies, have a duty to mitigate, to the extent practicable, any harmful effect known to the Covered Entity and / or Business Associate of a use or disclosure of PHI in violation of its policies and procedures or the requirements of HIPAA, HITECH and applicable regulations. If the Business Associate alone is aware of the breach, the Business Associate must report unauthorized uses, disclosures and security breaches to the Covered Entity. Many states also require notice to the affected individual in the event of improper use or disclosure of PHI.

A breach of PHI is defined as the unauthorized acquisition, access, use or disclosure of PHI which compromises the security or privacy of the PHI. "Unsecured PHI" refers to PHI that is not secured in accordance with certain technology or methodology specifically identified by the Department of Health and Human Services that makes the PHI unreadable, unusable or indecipherable to unauthorized individuals. At this time, "secured" involves either encrypting or destroying the PHI.

What To Do If A Breach Of PHI Occurs

If a breach does occur, the Covered Entity and / or the Business Associate must notify the affected individual (and the Business Associate must notify the Covered entity if the latter is unaware of the breach) within a reasonable amount of time but no later than sixty (60) days after the discovery of the breach.

Individuals must be notified promptly by first-class mail at the last known address of the individual or by electronic mail if the individual has agreed to such means. Notification must be on-going in one or more mailings as information about the breach becomes available.

If there is out-of-date or insufficient contact information regarding the individual whose PHI has been inappropriately used or disclosed, a substitute form of notice is deemed to be acceptable. For example, if there are ten (10) or more such individuals, a posting must be placed on the home page of the web-site of the Covered Entity and / or Business Associate involved or notice must be placed in major print or broadcast media in geographic areas where the affected individuals of the breach most likely reside. A toll-free telephone number should also be included in the media or web notices. Individuals can then call to determine if their PHI is included in the breach. Telephone calls may also be used to communicate notice to affected individuals if time is of the essence. If more than five hundred (500) individuals have been affected by the breach of unsecured PHI, notice must be provided to major media outlets serving the geographical area affected.

The Covered Entity must notify the Department of Health and Human Services (DHHS) of unsecured PHI that has been acquired or disclosed in a breach. If five hundred (500) individuals or more have been affected, then notice to DHHS must be immediate. If less

than five hundred (500), then the Covered Entity may maintain a disclosure log and submit such a log annually to DHHS.

The notice of breach must include the following:

- a brief description of what happened including the date of the breach and the date of discovery of breach;
- a description of the types of unsecured PHI involved in the breach;
- steps individuals affected by the breach should take to protect themselves from possible harm from the breach;
- a brief description of what the Covered Entity and / or Business Associate is doing to investigate the breach, mitigate losses and protect the individual from repeated breaches;
- means for the affected individual to ask questions or gather additional information including a toll-free telephone, a web-site, mailing address or e-mail address.

  For further information please contact us at:

  sfern@barmak.com

  609 454 5351

  609 454 361 FAX

  www.barmak.com