



Privacy and Security of Medical, Financial and Personal Information

April 2015

One only has to look at the headlines in any month to gain an understanding of the importance of maintaining privacy and security of personal information – medical, financial or otherwise. A data breach at an insurance company, hospital, retailer, or from a broker has far reaching consequences.

Insurance brokers, including their staff, create, maintain, use and transmit information that contains personal and medical information on a regular basis. Reflecting the sensitivity of this information, insurance brokers are subject to a myriad of laws and regulations to protect information. Among these are HIPAA, HIPAA-HITECH, state confidentiality and privacy laws and more.

There are also agreements brokers must enter into that contain restrictions and obligations in this regard. Brokers participating in the exchanges created by the Affordable Care Act (PPACA) agree to significant standards. Brokers working with insurance plans and related entities are contractually obligated to follow standards typically enumerated in a Business Associate Agreement (BAA). They in turn must have Agreements with vendors e.g. a company that may maintain files, TPAs, even with Microsoft, i.e. anyone who *maintains* such information. In addition to being costly, it does mean a great deal of education and remaining updated on laws and consequences of disclosure leading to breaches and lawsuits. Also paramount is the concern of facilitating identity theft by mishandling of information.

Regulation is only expected to increase, especially in light of the ongoing conversion of what were once paper records to digital records. **NAHU believes it is important to recognize the inherent risks of these records while supporting reasonable measures and responsibilities for brokers.**

Personal Health Information (PHI)

NAHU believes that individuals should have an expectation of confidentiality with respect to their personal health information and records. A patient who is fearful that his or her medical records might be disclosed without authorization to a third party may withhold medical information, give false information, or simply not seek treatment for his or her medical condition, resulting in a lack of proper medical treatment, the wrong treatment or no treatment at all.

NAHU believes that any entity or person obtaining PHI should be expected to take reasonable measures to secure this important information. This includes information in many forms including information that is maintained in paper records or electronic records.

NAHU believes that individuals have specific rights with respect to their medical records. **Individuals should be able to inspect or copy their medical records, to request an amendment to their medical records,** and to



Privacy and Security of Medical, Financial and Personal Information

April 2015

have a written copy of any disagreement they have with the content of their medical records listed as a permanent part of their medical file, if their request for amendment is denied.

NAHU acknowledges that law enforcement may have a legitimate use for medical records where an authorization for disclosure has not been made, for example, in the lawful interest of public safety when investigating a felony. **NAHU believes, however, that these uses should be the exception and not the rule, and that specific requirements for their use should be laid out in legislation**, to ensure only appropriate release of information.

Personally Identifiable Information (PII)

NAHU believes that individuals should have an expectation of confidentiality with respect to their personally identifiable information and records. Personally Identifiable Information (PII) is any information that can be used to distinguish or trace an individual's identity, alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual. Examples of PII include: name, Social Security Number, address, email and date of birth. All brokers have access to PII and must be mindful that it is also protected under HIPAA.

NAHU believes that any entity or person obtaining PII should be expected to take reasonable measures to secure this important information. This includes information in many forms including information that is maintained in paper records or electronic records.

Financial Records

Confidentiality of financial information should be regarded with the same diligence as medical records.

Conclusion

NAHU believes that the American consumer has a right to expect that those entities with access to their medical, financial, personal and other confidential records will take steps and exercise reasonable care to protect them.

NAHU believes that any entity or person obtaining such records should be expected to take reasonable measures to secure this important information. This includes information that is maintained in paper records or electronic records.

NAHU generally supports reasonable laws and regulations aimed at ensuring these expectations are met.