KROKIDAS & BLUESTEIN
ATTORNEYS
600 ATLANTIC AVENUE
BOSTON, MASSACHUSETTS 02210
PHONE 617-482-7211 • FAX 617-482-7212

CLIENT ALERT: MARCH 20, 2008

CMS PUBLISHES HIPAA SECURITY COMPLIANCE CHECKLIST

Recently, the Office of E-Health Standards and Services (OESS), within the Center for Medicare & Medicaid Services (CMS) of the U.S. Department of Health and Human Services (HHS), posted a document entitled "Information Request for Onsite Compliance Reviews" (the "Publication") to the section of the CMS website dedicated to the Health Insurance Portability and Accountability Act of 1996 (HIPAA). A copy of the Publication (released February 20, 2008) is attached.

OESS provides technical guidance about, and implements the enforcement program for, the **HIPAA Security Rule** (45 CFR Parts 162 and 164, Subpart C). OESS recently contracted with PricewaterhouseCoopers to assist with on-site HIPAA Security Rule compliance reviews ("Security Reviews") which will make use of this Publication. Security Reviews may be triggered by allegations of non-compliance received by CMS via complaints, the media, or self-reporting. These Security Reviews are separate from the independent review by the HHS Office of the Inspector General (OIG) of CMS's oversight, implementation, and enforcement of the Security Rule, which OIG review may include random audits of provider compliance.

Note that the HHS Office for Civil Rights (OCR) continues to implement the enforcement program for the **HIPAA Privacy Rule** (45 CFR Part 164, Subpart E). Although the Publication pertains to Security Reviews, the content of the guidance has relevance to Privacy Rule compliance as well.

With respect to Security Reviews, the Publication lists categories of personnel who might be interviewed and types of information that might be requested. The Publication highlights in particular several vulnerable areas associated with the security of electronic protected health information. Note that OESS indicated that the Publication is not a comprehensive list of review areas.

With respect to HIPAA compliance generally, the Publication serves as guidance as to which HIPAA policies and procedures providers might be expected to have in place. In light of this guidance, providers may wish to inventory their HIPAA policies and procedures, as well as their documentation of associated trainings conducted. A particular focus area might be security incidents because it is an area that also was recently regulated by Massachusetts law. (See

articles on our website concerning the new Chapters 93H and 93I of the General Laws at http://www.kb-law.com/news/index.php.)

Additional information concerning HIPAA Security Rule enforcement by OESS can be found at http://www.cms.hhs.gov/Enforcement/025_GeneralEnforcementInformation.asp.

CD\0001\221452.5