Society of Professional Benefit Administrators
Two Wisconsin Circle, Suite 670
Chevy Chase, MD 20815
Phone: 301-718-7722
Fax: 301-718-9440

ERISA Advisory Council

Hearing on Outsourcing Employee Benefit Plan Services

June 7, 2016

Testimony of

Kevin Schlotman

Vice President, Director of Employee Benefits

CAI Insurance Agency, Inc. and Benovation

Secretary/Treasurer, Society of Professional Benefit Administrators

Good Morning Members of the Council, DOL Staff and guests.

I am Kevin Schlotman, Vice President and Director of Employee Benefits of CAI Insurance Agency, Inc., located in Cincinnati, Ohio. CAI operates as a health insurance and employee benefits broker, and as a healthcare Third Party Administrator (under the name Benovation). I am here on behalf of the Society of Professional Benefit Administrators where I serve as Secretary Treasurer.

SPBA is the national association of Third Party Administration (TPA) firms that are hired by employers and employee benefit plans to provide contract-based management of their employee benefit plans. All the members of SPBA provide services to health plans and some also serve pension plans. Our comments today will focus on the cyber risks that benefit plans, particularly health plans, are exposed to, and steps that are being taken to manage those risks.

Executive Summary

Healthcare Plans need Protected Health Information and Personally Identifiable Information in order to operate. This fact makes them a target for Cyber attack. Health Plans would benefit from a clear, concise guide to help them evaluate their exposure to data breaches and Cyber crimes. Properly advised Health Plans already have a robust contractual risk transfer mechanism in place with their Business Associates. Marrying the HIPAA Security Rule Crosswalk to the NIST Cybersecurity Framework and the Business Associate Agreement and creating a user friendly checklist will help Health Plans evaluate their Cyber risk, and provide steps necessary to improve their Cyber security program.

Background

Health Plans, by nature, have access to information that qualifies as Personally Idenitifiable Information (PII) and Protected Health Information (PHI). Plan Sponsors of fully insured programs will generally have access to and must manage PII in order to manage eligibility for the members of their Plan. Self-Funded Plan Sponsors need to manage the PII associated with eligibility for benefits plus PHI in order to effectively and properly oversee the operation of their Plan. PHI data is far more valuable to Cyber criminals than credit card or even bank account information. As such, organizations that provide services to Health Plans – Insurers, Third Party Administrators, Wellness Program service providers, Pharmacy Benefit Managers, PPO Networks, Disease Management firms, etc. – should expect to be targets of Cyber criminals.

Direct threats include mishandling of PHI/PII by those entrusted to manage the Plan, theft or loss of physical assets containing PHI/PII (e.g. laptops, smart phones), information technology system breaches. Cyber criminals will attack network access points, conduct phishing expeditions, and social engineering attacks. It's clear that the threat to Health Plans is real, and must be addressed in order to protect Plan participants. The Cyber risks threatening Health Plans are the same, regardless of the number of covered participants.

Health Plans take various steps to counter the threat of data loss or systems breach. The very first step involves identifying the roles and responsibilities of the entities involved with the operation of the Health Plan.

The Plan is, according to HIPAA rules, a Covered Entity and is compelled to execute a Business Associate Agreement (BAA) with any organization with which it will share PHI/PII in order to operate the Plan – most typically a Third Party Administrator (TPA). The TPA may be an independent organization or owned by a large insurer. The BAA may be executed as an addendum to an Administrative Services Agreement, or as a separate contract. Execution of the BAA prior to commencement of services has been a standard practice for Health Plans for more than 10 years, though the BAA itself has evolved alongside the requirements of HIPAA (including HITECH). The BAA clearly delineates the responsibilities of the Plan and the Business Associate as they relate to the protection of data, communications containing PHI/PII between the parties, duties in the event of a suspected or verified breach, as well as the Business Associates responsibilities relative to any subcontractors it may utilize. The penalties for breach are defined by Federal and State Law, as are the penalties for failure to take proper steps in the event of a breach.

Health Plan Sponsors are keenly aware of the sensitive nature of the information that they need to operate their Plan. Properly advised, they take significant steps to protect any PHI/PII they receive. Distribution is limited to individuals that need the information in order to make sure that the correct benefits are provided to the right individuals. Even in the smallest Plans, steps are taken to separate duties to minimize the potential for the misuse of PHI/PII for employment decisions. Attention is given, and procedures implemented, to the proper distribution, transfer, and storage of PHI/PII.

Regardless of size and funding mechanism (fully insured vs. self-funding), Plan Sponsors rely on their service partners to protect their sensitive data. Informal (and unscientific) polling of health plans large and small (from 125 plan participants to 14,000+) indicates that this is the current reality. Service partners – TPAs as an example – often maintain all of the Plan's operating data, with access granted to authorized individuals for the operation of the Plan. Some Plans request information about Cyber security and data protection from prospective third party vendors prior to engagement. Many do not, in significant part because they do not know where to begin. An easy to comprehend and use guide would provide them a reference from which they could start.

The Health Plan IT/systems Cyber security measures are nearly always part of the organization's enterprise wide IT security program. The sophistication of these programs vary significantly from organization to organization. Certainly, industries that are heavily regulated (banking, healthcare, insurance) are farther along than others, like manufacturing or construction. This is true regardless of size, but is most pronounced for firms with less than 500 employees. While this is a reliable rule of thumb, it must be treated as a guideline, not a rule. It's certainly true that an IT consulting firm with 75 employees is likely to have a robust Cyber security program, as well as a more thorough vender Cyber risk vetting initiative. Regardless, the Enterprise wide Cyber risk management program includes the Health Plan. There is generally not a separate program for the operations of the Health Plan.

The structure to create valuable and viable guidance to Healthcare Plan Sponsors largely exists. The HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework is a suitable starting point. Most Plan Sponsors would benefit from a condensed checklist based on this already published crosswalk. A condensed and easy to follow checklist would be valuable to Healthcare Plan Sponsors, regardless of the number of Plan Participants. Any checklist should emphasize a Cyber security training program that includes every employee, including new hires. Training for employees expected to encounter PII/PHI should be more detailed and cover breach responsibilities and methods to safeguard communications with external service partners. Any such training program should work in concert with an evaluation of the operation of the Healthcare Plan, and perhaps the enterprise as a whole, according the the HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework. This training program, comprehensive evaluation, and the execution of an appropriate Business Associate Agreement will permit the Plan to identify their exposure to Cyber Risks, as well as provide a roadmap to mitigate those risks.

I appreciate the opportunity to provide this testimony and hope that it will serve to further the Council's stated objective of assisting Health Plans to idenitfy and address their Cyber risks. Please do not hesitate to contact me to discuss this topic further, or if I can be of any further assistance.