THE ERISA INDUSTRY COMMITTEE

1400 L Street NW, Suite 350, Washington DC 20005 (202) 789-1400 fax: (202) 789-1120 www.eric.org
Advocating the Benefit and Compensation Interests of America's Major Employers

June 8, 2005

Chairman Rothstein, members of the Subcommittee on Privacy and Confidentiality, ladies and gentlemen, good morning, I am Edwina Rogers, vice president for health policy at the ERISA Industry Committee (ERIC). On behalf of ERIC and all of our members, thank you for allowing us this opportunity to give input on issues pertinent to privacy in health information technology.

Who We Are: ERIC is a nonprofit trade association committed to the advancement of employee retirement, health, incentive and compensation plans for America's major employers. ERIC members provide benefits to tens of millions of active and retired workers and their families.

Overview Of Issues: The widespread adoption of electronic medical records will be a boon for the US healthcare system, increasing efficiency and accuracy, while decreasing paperwork and aggravation. Electronic records also pose challenges for the system, and to major employers there are important issues that must be addressed under the Employee Retirement Income Security Act (ERISA) and the Health Insurance Portability and Accountability Act (HIPAA. Major employers will need access to these electronic records and to whatever system is devised so they can continue to deliver state-of-the-art health benefits to their employees, but today we must look at the privacy and security concerns these changes will bring.

The Challenges We Face: In the process of transitioning to a system of secure electronic health records, large employers that provide health and wellness benefit plans to their employees have a significant and difficult role to play. The current state of laws governing both medical data and benefit plans make for a great burden on companies that voluntarily provide medical coverage for their employees – one company may be subject to different laws in every state, it may be unclear as

to which of those state laws are preempted by federal laws, and it may be unclear as to which standards of privacy and security one must adhere. But the confusion and frustration are not as compelling as the desire employers have to maintain healthy employees.

ERISA – The Corrosion Of Exemption: To the extent that employer-provided health plans are subject to Title I (the Department of Labor Requirements) of ERISA, ERISA §514 preempts state laws "relating to" an employee benefit plan. However, laws relating to insurance, banking, or securities matters are "saved" from ERISA preemption under ERISA 514(a) and (b). The term "state laws" includes all laws, decisions, rules, regulations, *et cetera*.

However, the ERISA preemption power that allows the federal government to set the standards governing employer-sponsored benefit plans has been severely eroded in the wake of several court decisions that have led to a distinction between "partial" ERISA preemption and "complete" ERISA preemption. As you can imagine, the key here is the interpretation of which state laws "relate to" an employee benefit plan. Under current case law, even state laws that may pertain to benefit plans, but are not related to ERISA benefits due to a participant *per se*, may not be preempted by ERISA. While these partial and complete preemption concepts are an important part of fully understanding ERISA preemption, the distinction between these concepts is not as important as the fact that the law has evolved to see fewer state law claims preempted by what was once thought of as an expansive ERISA preemption doctrine.

To simplify (and perhaps over -simplify) the state of ERISA preemption today, one could draw from the case law that claims brought under ERISA §502(a), to recover benefits due under the terms of the plan, are completely preempted by ERISA – for example, an employee's state breach of contract claim against an employer who fails to provide benefits due under the health plan will fail due to ERISA preemption under current law. Furthermore, state claims that are related to the plan, but are not for benefits *per se*, may not be preempted by ERISA under the partial preemption

doctrine. Be aware, however, that this is a vast oversimplification of the law. ERISA law regarding preemption is very convoluted and uncertain; there are few bright line rules, and several jurists have called on Congress to set clear ERISA preemption boundaries.

ERISA Preemption And Electronic Records: If ERISA is amended to mandate that employee benefit plans transfer health data electronically to health providers, there is question as to whether more stringent state privacy laws could bar or severely restrict this practice or would ERISA preempt. You also have this problem with the privacy rules under HIPAA, because Section 264(c)(2) of HIPAA provides that contrary State laws that relate to the privacy of individually identifiable health information will not be preempted by the federal requirements if they are "more stringent" than those requirements. This means that HIPAA's federal privacy protections act as a floor, not a ceiling, on privacy protections – state laws cannot lower the standards, but can be more restrictive.

In contrast, federal laws mandating the transfer of health data electronically should have a ceiling, and inconsistent state laws that would inhibit this practice would need to be preempted to ensure the objectives of such laws will be met. However, given that the scope of ERISA preemption is being narrowed and not widened, there is an increasing chance that ERISA's current preemption provisions will not suffice to preempt state privacy laws once current case law interpretation is applied. Because one could argue that such state laws regarding health care privacy rights relate to the plan, but are not related to benefits *per se*, such laws may not be preempted by ERISA under the Courts' current interpretation of the law. Therefore, we strongly argue for one national standard that includes ERISA plans and preempts all state laws.

The HIPAA Dilemma: The millions of Americans employed by large employers constantly have their health plans threatened by overzealous State laws that go above and beyond HIPAA base requirements in varying ways. Because there is not a uniform standard but rather, simply a uniform base, and different and more stringent state standards, varying widely by state, an employer who

operates in multiple states may find it necessary to conform coverage in all states to the strictest privacy and security standards available. While this may sound positive, in fact it amounts to a waste of time, resources, and legislation – after all, if the federal HIPAA standards are not sufficient to protect patients' medical records, why should HIPAA even exist as a standard?

It is more than likely that the transition to a system of electronic health records will face its most burdensome barrier in the form of varying state privacy laws. For example, a Texas-based company may be eager to achieve the administrative and efficiency cost-savings inherent in moving to electronic health records, they will have to thoroughly examine whether the specifics they develop will be legal in Maine, Iowa, and 47 other states. Some concerned parties are turning to accrediting organizations to help them achieve compliance with the tangled privacy legislation currently on the books, organizations like the Utilization Review Accreditation Commission (URAC).

URAC's HIPAA Privacy and HIPAA Security accreditation programs outline a framework of best practices that describe the operational policies and procedures necessary for an effective compliance program, and are designed to accredit many different types of health care organizations including both plan sponsors and payers. URAC accreditation demonstrates good faith efforts to meet HIPAA requirements to current and potential business partners and assures customers and patients that appropriate steps are being taken to safeguard protected health information. HIPAA itself is so unclear and conflicted when faced with state laws and regulations that companies often have no idea whether or not their efforts to comply have been successful – thus necessitating the help of outside experts who can evaluate whether or not they have put in good faith efforts. It would be too much to decide whether or not a company was actually completely in compliance – that would remain anyone's guess, considering the changing state laws.

Employers Play A Critical Healthcare Role: Employers have two reasons for providing voluntary healthcare benefits to their employees – they desire both to attract the best employees by offering

the best compensation and benefits, and also to retain healthy employees that don't succumb to illness, which would lead to absences and a loss of productivity. While the first goal can be accomplished simply by pursuing the most efficient and accommodating plans, the second has lead employers to get intimately involved in their employees' healthcare.

In order to keep employees healthy, some companies started buying outside fitness center memberships for their employees. This has lead to less outsourced methods being used, including companies providing their own health and fitness facilities for employees. And why stop there – large employers now often offer employees their own pharmacies, drug therapy centers, smoking-cessation programs, obesity-curbing programs, and other health and wellness amenities that both help employees stay healthy and also increase the necessity of employers having access to their employees' medical records and histories. This health information must be kept confidential and contained; meaning that other parts of the employer company may not have access to the health records which the pharmacy and drug therapy units will have access. We are not aware of any health record breaches by major employers.

ERIC's Conclusion: While there is the distinct possibility that a new medium for medical information will require increased vigilance and new means of procuring security, it is likely that employers will be more than willing to make accommodations in order to best serve their employees. The key to instituting a successful transition to electronic records will be including employers – and in doing so, helping them comply with security and privacy necessities by creating uniform standards that are not the baseline, but the end-line. Employers are involved in many aspects of health care, and they require clear, concise goals and rules in order to accurately deliver the services their employees are demanding. Please contact me at (202) 789-1400 or erogers@eric.org if we can be of assistance. ERIC often surveys its members regarding benefit designs and wellness programs, and we could conduct such a survey for this committee if requested.