

## **THE REGULATION OF SELF-INSURED HEALTH CARE PLANS – HIPAA PRIVACY AND SECURITY RULES GREATLY INCREASE THE REGULATORY BURDEN ON EMPLOYERS**

Glennon J. Karr, Esq.  
614.848.3100

One of the real advantages of having a self-insured Health Care Plan in the past has been the ability to avoid a lot of regulation of the Plan at the state and federal levels. The Employee Retirement Income Security Act (ERISA)<sup>1</sup>, through its preemption of state law provision, has allowed large and medium sized companies who choose to self-insure their Health Care Plan to avoid all of the state mandates required in each state's insurance codes – examples include mandating payments to certain types of providers, like chiropractors, or paying minimum amounts of coverage for certain mental health types of benefits. Each state has those statutes, and because ERISA preempts them, multi-state companies can have a uniform self-insured Health Care Plan that doesn't need to change from state to state. Mandated benefits, which vary from state to state, limit the flexibility of Plan designs. Because state mandates have been avoided, and because until recently mandates at the federal level were few, self-insured Health Care Plans have had a lot of freedom to determine the types of benefits to include (or not to include) and how other features of the plans would be handled. The various regulatory laws in each state in which the plan operates are typically avoided entirely.

In the past several years, however, regulation of self-insured Health Care Plans has increased – but the increased regulation has come at the federal level. COBRA (The Consolidated Omnibus Budget Reconciliation Act of 1985<sup>2</sup>), as amended, was the most notable first new regulatory action. It requires companies to extend coverage when a plan participants' coverage would have otherwise ended due to employment termination. That law required some additional paperwork and compliance, but this was often contracted out to companies that handled COBRA benefits for the company, typically to the third party administrator that handled claims payment. In the late 1990's additional new federal regulatory measures became effective. The Mental Health Parity Act of 1996<sup>3</sup> was enacted. That law is actually misnamed. Although it purports to equalize mental health benefits with benefits provided for physical health conditions, it merely changed the way those plans had to be designed. In order to get the law passed, the Clinton Administration, along with a Republican Congress, developed legislation that appeared to provide for mental health parity, but which actually ensured no effective change. The law doesn't require that a Plan provide mental health benefits and there is no requirement for consistency in deductibles or co-payments between mental and physical health conditions. It did, however, require most Health Care Plans offering mental health benefits to change their benefit designs in order to comply. For instance, it made placing an annual dollar limit on coverage for inpatient and outpatient benefits unlawful if those limits applied only to mental health treatment and not to physical conditions, but specifically allowed the outpatient visits or inpatient stays to be capped at a limited number of visits or days, at limits inconsistent with visits to a medical doctor or a hospital stay for a physical condition. So the Plans were redesigned to comply with the new law's exceptions and the benefits effectively stayed the same, treating mental and physical conditions with two different sets of benefit limits.

ERISA has always had specific requirements which must be met in regard to how the Summary Plan Description (which describes the benefits of a Plan) is prepared<sup>4</sup>. There are notices which must be filed when changes to the Plan are made. There were additional regulatory requirements in the Newborns' and Mothers' Health Protection Act<sup>5</sup>, passed in 1996, which mandated minimal hospital stays involving the birth of babies. The Health Insurance Portability and Accountability Act of 1996<sup>6</sup> was originally intended to provide for portability of plans when an employee left a company and was seeking insurance at a new company. It reduced the ability of insurance companies to apply pre-existing condition exclusions on employees. And then the breast cancer lobbying group was successful in passing a law in 1998 which requires a yearly notification that there are certain rights where breast cancer is involved (The Women's Health and Cancer Rights Act<sup>7</sup>), as well as minimal coverage for certain procedures involving women's cancer.

Although these laws provided more Plan regulation, they were generally not too onerous to follow. Then came the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule<sup>8</sup>, which was effective for larger self-insured Plans on April 14, 2003, and for small self-insured Health Care Plans (those with receipts of \$5 million or less per year<sup>9</sup>) a year later<sup>10</sup>. On April 21, 2005, the Security Rule<sup>11</sup> became effective for the larger self-insured Plans, followed a year later by the smaller Plan's effective date. Also to be noted is that the Privacy Rule only

applies to self-insured Health Care Plans covering 50 or more participants or any employer health plan that contracts with a third party administrator to handle claims payment<sup>12</sup>. Up until ten years ago it was unlikely that an employer with as few as even 100 employees would find establishing a self-insured arrangement cost-effective, and there are probably very few below the level of 50 participants that exist, particularly with the requirement that the employer must pay claims and can't hire a third party administrator to do that. So the exemption does not apply to very many plans, effectively making almost all self-insured employer Plans subject to HIPAA Privacy and Security Rules.

At this point, operating a self-insured health care plan is no small undertaking, mainly due to the regulatory requirements of complying with the HIPAA Privacy and Security regulations. Whereas previously a third party administrator could handle most of the functions for the employer, now the employer as the Plan Sponsor is largely responsible for complying with a whole new set of standards, rules, and regulations as a Covered Entity<sup>13</sup>. Each employer must audit their compliance on a regular basis, and it has substantially increased the cost of administering a self-insured Health Care Plan. The third party administrator, although still largely responsible for claims processing, cannot perform the functions that an employer must perform in order to comply with HIPAA. In fact, the third party administrator is not even directly regulated by HIPAA, it is only considered a "Business Associate"<sup>14</sup> of the Health Care Plan and its compliance obligations only arise out of a contract between the Health Care Plan and the third party administrator called a Business Associate contract.

The general definition of Protected Health Information (PHI) under HIPAA is quite broad and applies to almost all information in any way dealing with a person's past, present or future mental or physical health.<sup>15</sup> As a result, how information is handled within the employment setting has been substantially changed. One of the exceptions to HIPAA is an exclusion for employment records<sup>16</sup>. In other words, HIPAA does not apply to records held by an employer strictly in its role as an employer. Another exclusion involves workers compensation records<sup>17</sup>. If the employer has a self-insured Health Care Plan, the employer has to strictly separate out the functions involving the Plan from the rest of the human resource activities. For smaller employers which have one person handling the Health Care Plan as well as the rest of the human resource functions, the job functions have to be structured in such a way that the PHI does not flow from the Health Care Plan to the human resource activities. A smaller employer may have to transfer human resource functions from the human resource manager, who also handles the Health Care Plan issues, whenever a Health Care Plan issue is potentially involved in a human resource matter. If, for example, an employer has information on an employee's health condition through a workplace drug testing program, i.e. through a program not related to the Health Care Plan, that knowledge would not be affected by HIPAA and the employer could take action against the employee if there was a positive drug test for heroin. If however, while acting as the claims manager and decision maker for a self-insured Health Care Plan the employee learns that an employee was seen at an emergency room for a heroin overdose, the company is not allowed in any way to utilize that information for employment purposes. When PHI, i.e., the Health Care Plan information involving treatment of the heroin addiction, is within the Health Care Plan, it requires the employer to obtain a written Authorization from the employee in order to disclose that information to the employer in its role as an employer.

The Health Care Plan must have a policy manual directing how PHI is protected and handled, training sessions for all involved employees, a Notices of Privacy Practices form which spells out how the Plan handles information as well as the rights of the employee to have his or her information protected, and a complete set of forms for implementing the Privacy Rule. The Employer has to implement a complaint procedure, appoint a Privacy Officer, maintain a record of all disclosure of PHI outside of information used for treatment, payment or health care operations, and must otherwise follow the procedures it has adopted. The Plan must enter into Business Associate contracts with entities performing functions on behalf of the Health Care Plan, such as with an auditor, an attorney, or a third party administrator, and the performance of those parties must be monitored to ensure compliance with the Privacy and Security Rules, with action taken if there is a violation resulting in the unauthorized disclosure of PHI.

The HIPAA Security Standards provide for regulation and compliance of all electronically transmitted PHI, whether within the employer's health care operation or outside to a third party administrator, insurance agents, and others involved in handling Health Care Plan information. Each employer must perform frequent audits to determine how electronic information is handled and protected. For example, e-mails containing PHI must be encrypted or otherwise secured. Generally, the Security Rule provides for Administrative Safeguards, e.g., a data backup plan, or a plan to limit access through the use of a particular access authorization system, Physical Safeguards, e.g., a facility security plan which would provide for all computer equipment containing PHI to be kept in a locked room with limited access, and Technical Safeguards, e.g., automatic logoff of a computer when it is not in use and encryption

for the transmission of records.<sup>18</sup> Policies must be developed and implemented specific to the employer to cover all of these areas.

If PHI is somehow disclosed outside of the Health Care Plan, HIPAA has specific penalties that may apply. Although HIPAA itself does not provide a private right of action to sue for a violation, various state laws and/or court decisions do provide such a right. For instance, in September 1999, the Ohio Supreme Court, in *Biddle v. Warren General Hospital*<sup>19</sup> created new torts in Ohio, one for the unauthorized disclosure of confidential medical information and one for inducing the unauthorized disclosure of confidential medical information. The General Counsel for the Warren General Hospital system had requested intake forms to review for possible payments by a federal reimbursement program. The Ohio Supreme Court allowed the lawsuit to proceed against both the law firm and the hospital on the basis of these new torts. Each state's laws and court decisions must be checked to see the types of remedies and causes of action available when PHI is released without proper authorization.

So far, in terms of federal enforcement, patient privacy complaints have not resulted in drastic action. The Columbus Dispatch reported on June 11, 2006 that out of 20,124 complaints received by the U.S. Department of Health and Human Services' Office of Civil Rights up to that date and since the Privacy Rule became effective, only two people had been criminally prosecuted. In addition, not one fine had been levied against a hospital, a clinic, a pharmacy, a doctor, or an employer operating a self-insured Health Care Plan. However, new procedures to handle administrative fines and an appeals process are now in place. These were set forth in a Final Rule of the Department of Health and Human Services in February 2006<sup>20</sup>. Penalties of not more than \$100 may be imposed for each violation of the Privacy and Security Rules, while the total amount imposed for all violations of an identical requirement or prohibition during a calendar year may not exceed \$25,000. The Final Rule provides for an administrative procedure where contested violations can be heard by an administrative law judge. It is important to note, however, that in the preamble to the Final Rule that the Office of Civil Rights reaffirms its approach to achieve compliance through informal resolution of complaints. This should not give comfort to the employer who basically ignores its obligations to comply with the many and varied regulations that are set forth in the Security and Privacy Rules, since the employer may still be exposed to private causes of action, depending on the particular states laws and court decisions where the breach occurs.

A possible benefit from all of this is that there are now uniform standards for protecting confidential medical information. As the health care industry attempts to go paperless in the next ten years, which will inevitably involve exchanging information with employers (so long as the health care system is in large part an employer based system), the goal will be to protect the information to the greatest extent possible. Employers who have complied with all of the HIPAA requirements will have put processes in place that will ensure the protection of that information, processes that will most likely extend to other areas of the workplace where confidential employee information is involved. That could, ultimately, reduce their potential liability involving the release of any confidential employee information. However, operating a self-insured Health Care Plan, which was once a simple operation handled mainly by a third party administrator on a low cost basis, has now become a much more burdensome endeavor, mainly because of regulation at the federal level.

### *Endnotes*

<sup>1</sup> 29 U.S.C. Chp. 18

<sup>2</sup> IRC Sec. 4980(B), Title 26, Subtitle D, Chapter 43 U.S. Code

<sup>3</sup> 29 USC § 1185a

<sup>4</sup> 29 USC § 1022

<sup>5</sup> 29 USC § 1185

<sup>6</sup> 29 USC § 1181

<sup>7</sup> 29 USC § 1185b

<sup>8</sup> 45 CFR Parts 160, 164

<sup>9</sup> 45 CFR § 160.103

<sup>10</sup> 45 CFR § 164.534

<sup>11</sup> 45 CFR Parts 160, 164

<sup>12</sup> 45 CFR 160.103

<sup>13</sup> 45 CFR. §160.103

---

<sup>14</sup> 45 CFR § 160.103

<sup>15</sup> 45 CFR §160.103 and 45 C.F.R. §164.501

<sup>16</sup> 45 CFR § 164.501

<sup>17</sup> 45 CFR § 512

<sup>18</sup> 45 CFR § 164.304

<sup>19</sup> *Biddle v. Warren Gen. Hosp.*, 698 N.E.2d 1007 (1999)

<sup>20</sup> Federal Register, February 16, 2006 (45 CFR Part Subparts C, D and E)