

BRIEFINGS

INSIDE THIS ISSUE:

- Fair Pay Act
- Recovery Act Privacy Legislation
- Preemption for Medical Devices
- FTC On Behavioral Ads

The New Administration Affects “Change” By Enacting The Ledbetter Fair Pay Act

By: Ciara Ryan Frost, Jodi R. Marvet

On January 29, 2009, President Obama signed his first bill into law – the Lilly Ledbetter Fair Pay Act of 2009 (the “Ledbetter Act.”) The Ledbetter Act is designed to redress the perceived injustice inherent in the United States Supreme Court’s decision in *Ledbetter v. Goodyear*, 127 S. Ct. 2162 (May 29, 2007).

Lilly Ledbetter was employed by Goodyear as a plant manager for almost 20 years. Shortly before she retired in 1998, she received an anonymous tip that Goodyear was paying her less than her male counterparts. Accordingly, she sued Goodyear for sex based pay discrimination. Ledbetter alleged that, because of her sex, she had received poor evaluations and less favorable pay raises than her male counterparts throughout her employment with Goodyear. She contended that the past discriminatory pay decisions had a continuing affect on her pay, such that, towards the end of her employment, she was paid significantly less than her male co-workers. Goodyear argued that Ledbetter’s suit was time barred because she had not filed an EEOC charge within 180 days of its allegedly discriminatory pay decision. Ledbetter disagreed, arguing that a new pay discrimination cause of action accrued each time she received a paycheck.

On May 29, 2007, the Supreme Court rejected (by a slim majority) the “paycheck accrual” rule and held that the limitations period for filing an EEOC charge of Title VII pay discrimination begins to run on the date the allegedly discriminatory pay decision is made and communicated to the employee, not on the date each subsequent pay check is issued. Accordingly, the Court held that Ledbetter’s pay dis-

crimination claim was time barred. In a vigorous dissent, Justice Ginsburg implored Congress to correct “this Court’s parsimonious reading of Title VII” which she maintains is at odds with Title VII’s “broad remedial purpose.” Justice Ginsburg and many others deem the Supreme Court’s ruling unjust because pay disparity can take place over time and the discrimination may not be apparent immediately.

Congress heeded Justice Ginsburg’s call to action by passing the Ledbetter Act. Under the Ledbetter Act, an employee or any other individual (such as an employee’s spouse) who is “affected by” “a discriminatory compensation decision or other practice” may file a charge of discrimination against the employer. Specifically, the employee or other affected individual may file a charge of discrimination for up to six months after any of the following dates: (1) the date of the “discriminatory compensation decision or practice was adopted”; (2) the date the employee became “subject to” the challenged decision or practice; or (3) the date the employee is affected by the application of the challenged decision or practice, “including each time wages, benefits or other compensation is paid.” Thus, the Act applies not only to wages, but also to “benefits and other compensation.” Accordingly, retirees receiving pension benefits may use this language to argue that their pension benefits are insufficient because they are linked to discriminatory wages. The employee or other affected individual can recover back pay and benefits for a period of up to 2 years preceding the filing of the charge.

Notably, the Ledbetter

[Continued on Page 3](#)



JUMP START ON PRIVACY - THE AMERICAN RECOVERY AND REINVESTMENT ACT ADDRESSES HIPAA AND NOTIFICATION ISSUES

PEGGY REETZ

The recently signed American Recovery and Reinvestment Act includes updates on safeguards regarding medical information. Title XIII of the law, entitled the “Health Information Technology for Economic and Clinical Health Act” or the “HITECH Act” is the section that addresses new appropriations and requirements for health information technology (“HIT”). The section contains modifications to privacy and security rules under the Health Insurance Portability and Accountability Act (“HIPAA”). The Act prohibits the sale of medical records, with exceptions for research, public health and treatment. The Act also limits marketing, requires covered entities and businesses to keep an audit trail of disclosures, mandates policies setting standards for technology systems, updates penalties for HIPAA violations and outlines data breach notification requirements.

The Act establishes authority in a National Coordinator of HIT policy whose objectives include: the electronic exchange and use of health information and the enterprise integration of such information; the utilization of an electronic health record for each person in the United States by 2014; the incorporation of privacy and security protections for the electronic exchange of an individual’s individually identifiable health information; ensuring security methods to ensure appropriate authorization and electronic authentication of health information and specifying technologies or methodologies for rendering health information unusable, unreadable, or indecipherable.

While there are updates and enhancements to HIPAA, the Act specifies that with respect to HIPAA privacy and security law, the Act has no effect on the authorities of the Health and Human Services Secretary under HIPAA and the purposes of the Act take into account HIPAA.

Breach Notification

Similar to data breach notification statutes enacted by a majority of states, the Recovery Act now requires notification of breaches involving protected health information (“PHI”). The Act states, “A covered entity that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured protected health information ... shall, in the case of a breach of such information that is discovered by the covered entity, notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, or disclosed as a result of such breach.” (State statutes typically identify residents of their states as those to receive such notification).



A Business Associate shall, following the discovery of a breach of protected health information, notify the covered entity. The notice shall include the identification of each individual whose unsecured PHI has been or is reasonably believed to have been accessed/disclosed. A breach is considered discovered on the first day on which a breach is known to either a covered entity or business associate (including employees, officers, agents). The notifications shall be made “without unreasonable delay” and in no case later than 60 calendar days after discovery (delays allowed for cooperation with investigative or federal security authorities).

The notification provisions are effective 30 days following the issuance by the Secretary of interim final regulations, which are to be completed within 180 days after the date of the enactment.

Business Associates

The Act now establishes that civil and criminal penalties applicable to a “covered entity” as defined under HIPAA will likewise apply in the same manner to a business associate that violates any security provision of HIPAA. Previously, business associates need only be compliant with such obligations further to contracts with the covered entity. Vendors of personal health records (“PHR”) also are subject to breach notification requirements.

Minimum Necessary for PHI Disclosure

Current regulations outline that covered entities are required to use, disclose and request only the “minimum necessary” PHI. The Act directs the HHS Secretary to issue guidance on “minimum necessary” within 18 months. In the case of the disclosure of protected health information, the covered entity or business associate disclosing such information shall determine what constitutes the minimum necessary to accomplish the intended purpose of such disclosure.

Audit Trail

If a covered entity or business associate uses or maintains an electronic health record with respect to protected health information, an individual shall have a

Continued on Page 4

WISCONSIN SUPREME COURT FINDS STATE LAW TORT CLAIMS PREEMPTED

TERRY HACKETT

On February 17, 2009, the Wisconsin Supreme Court held that the express preemption provision of the 1976 Medical Device Amendment to the Federal Food, Drug and Cosmetic Act, preempted the negligence, strict liability and loss of consortium claims asserted by plaintiffs claiming injury from a Medtronic implantable cardioverter defibrillator. *Blunt v. Medtronic*. Before selling the device, Medtronic sought and obtained "pre-market approval" for this Class III medical device from the FDA. Pre-market approval is required for such devices and, according to the United States Supreme Court, is a rigorous process evaluating issues relating to the safety and effectiveness of the device. Defendants argued that because the FDA approved the device through the pre-market approval process, a state law tort claim would constitute state requirements different from, or in addition to, the federal requirement. The Wisconsin Supreme Court agreed with the Defendants and applied the United States Supreme Court's analysis in *Riegel v. Medtronic* to find express preemption based upon the pre-market approval. The trial court and the intermediate appellate court also found Plaintiffs' claim in *Blunt* were preempted.

The Plaintiffs in *Blunt* tried to distinguish *Riegel* by arguing that a subsequent pre-market approval of a new and improved cardioverter defibrillator negated the preemption analysis for the device at issue in the case. The Wisconsin Supreme Court rejected that analysis as unsupported by the comprehensive federal regulatory scheme.

Blunt and *Riegel* are two of several recent cases addressing preemption. In a 5-4 decision of the U.S. Su-



preme Court on December 15, 2008, in *Altria Group, et al. v. Good*, the Court found that the Federal Cigarette Labeling and Advertising Act ("FCLAA") did not preempt a claim by some Maine residents that Altria violated the Maine Unfair Trade Practices Act. In that case, the plaintiffs claimed that Altria's advertising fraudulently conveyed the message that their "light" cigarettes deliver less tar and nicotine to consumers than "regular" cigarettes despite Altria's knowledge that the message was untrue. The Court held that, based on prior precedent and the wording of the FCLAA, the language of the FCLAA was not broad enough to include these state law tort claims and therefore they were not preempted. The majority reiterated the assumption that the historic police powers of the states are not to be superseded by a federal law "unless that was the clear and manifest purpose of Congress."

Also, in November 2008, the United States Supreme Court heard argument on a third preemption case, *Wyeth v. Levine*. The issue in *Wyeth* is whether an FDA mandated warning relating to the administration of the drug Phenergan preempts state law tort claims. In *Wyeth*, the plaintiff had her arm amputated after it turned gangrenous when she was administered Phenergan through an IV push. The FDA-approved warning label warns against this possible complication, but does not warn that an IV push of Phenergan is prohibited. On March 4th, 2009, the court issued a 6-3 decision finding that the state law failure to warn claim in that case was not preempted by the FDA's prior approval of the warning label.

FAIR PAY ACT (CONT'D)

Act applies not only to Title VII claims for discrimination based on race, color, religion, sex or national origin, but also to claims under the Age Discrimination in Employment Act, the Americans with Disabilities Act, and the Rehabilitation Act of 1973. The law applies retroactively to all pay discrimination claims "pending" on or after May 28, 2007, the date of the *Ledbetter* decision.

By expanding the pool of potential claimants as well as the period of time in which claimants can bring claims, the *Ledbetter* Act will likely increase both the frequency and severity of employment discrimination claims.

right to receive an accounting of disclosures (for a period of 3 years preceding). In response to a request for an accounting, a covered entity shall provide either an accounting of PHI disclosures that are made by the covered entity or business associate or a list of business associate contact information. A business associate shall provide an accounting if a request is made by the individual directly.

Sale /Marketing of PHI

With certain exceptions, there is a prohibition on the sale of electronic health records or protected health information by a covered entity or business associate (no direct or indirect "remuneration in exchange for any protected health information"). The exceptions address transmittal costs, costs for the purpose of treatment and other scenarios. The Secretary again is directed to issue guidelines on appropriate exceptions. Marketing is not considered a "health care operation" under this section and thus the prohibition on the exchange of electronic health records or PHI applies.

Encryption

When individually identifiable health information is transmitted or physically transported



outside a health care entity, it must be encrypted or otherwise indecipherable to unauthorized person.

Enforcement

The Attorney General in any state where residents are threatened or adversely affected by a violation of these provisions may bring a civil action on behalf of such residents to enjoin activity or obtain damages.

The Act updates penalty provisions. Fines range from \$100 per violation to a maximum of \$1.5 million for violations in a calendar year. There is a "tiered" system based on a person's knowledge, reasonable cause or willful neglect. The new penalty amounts may not apply if there is a correction within 30 days. The penalties would apply to violations after the date of enactment.

Updates by the HHS Secretary will be closely watched for additional impact on entities and types of information affected.

Briefings is published solely for the interests of friends and clients of Kerns, Frost & Pearlman and should in no way be relied upon or construed as legal advice. For specific information on recent developments or particular factual situations, the opinion of legal counsel should be sought. Kerns, Frost & Pearlman is a limited liability company. Copyright © 2009 Kerns, Frost & Pearlman.

Chicago

Three First National Plaza
70 West Madison
Suite 5350
Chicago, Illinois 60602
Telephone: (312) 261-4550
Fax: (312) 261-4565

Bannockburn

2201 Waukegan Road
Suite E-200
Bannockburn, Illinois 60015
Telephone: (312) 261-4570

You have received this email because you are on the firm's distribution list. This message is sent by a law firm and may contain information that is privileged or confidential. If you have received this transmission in error, please notify the sender by reply email and delete the message and any attachments. These materials may be considered ATTORNEY ADVERTISING in some states.

© 2009 All Rights Reserved. Kerns, Frost & Pearlman. For additional information, please visit our website at www.kpfplaw.com

FTC Staff Outlines Online Behavioral Advertising Principles

On February 12, 2009, the FTC staff issued a report describing its examination of online behavior advertising. The concern as noted by the staff is how to protect consumers' privacy while advertisers collect information about their online activities. The current report discusses whether it is necessary to provide protections for data that is not personally identifiable. The report states that privacy protections should cover any data that reasonably can be associated with a particular consumer or computer or other device.

The report concludes that fewer privacy concerns may be associated with "first-party" behavioral advertising (in which a Web site collects consumer information to deliver targeted advertising at its site but does not share any of that information with third parties) and "contextual" advertising (which targets advertisements based on the Web page a consumer is viewing or a search query the consumer has made, and involves little or no data storage).

Noting that privacy policies posted on companies' Web sites often are long and difficult to understand, the report encourages firms to design creative and effective disclosure mechanisms that are separate from their privacy policies. The report also states that companies that collect information outside the traditional Web site context – for example, through a mobile device or by an Internet Service Provider – should develop disclosure mechanisms that are meaningful and effective for these contexts. See, <http://www.ftc.gov/opa/2009/02/behavad.shtm>