



STATE OF ARKANSAS
**Department of Finance
 and Administration**

EMPLOYEE BENEFITS DIVISION

501 Woodlane, Suite 500
 Little Rock, AR 72201-1011
 Post Office Box 15610
 Little Rock, AR 72231-5610
 Phone: (501) 682-9656
 Toll Free: (877) 815-1017
<http://www.arkansas.gov/dfa/ebd>

September 1, 2009

To: Health Insurance Representatives

From: EBD Compliance

Subject: HIPAA Changes

As many of you already know, The American Recovery and Reinvestment Act of 2009 was signed into law in February.

This new law has had quite an impact on health insurance, including changes to COBRA and HIPAA.

Since most of the recent focus has been on the changes to COBRA, we wanted to make sure that you are all aware of the changes to HIPAA and how it impacts you as a Business Associate.

One of the major changes that took effect on February 17, 2009, was the immediate increase in monetary penalties that can now be applied **directly** to the Business Associate. The grid below shows the current penalties that can be levied under HIPAA.

Circumstance of Violation	Minimum Penalty	Maximum Penalty
Entity did not know (even with reasonable diligence)	\$100 per violation (\$25,000 per year for violating same requirement)	\$50,000 per violation (up to \$1,500,000 annually)
Reasonable cause, not willful neglect	\$1,000 (\$100,000)	\$50,000 (up to \$1.5 million annually)
Willful neglect, but corrected within 30 days	\$10,000 (\$250,000)	\$50,000 (up to \$1.5 million annually)
Willful neglect, not corrected	\$50,000 (\$1,500,000)	none

Additionally, the State Attorney General can now enforce HIPAA's privacy and security requirements. The Attorney General may sue the suspected violator in Federal District Court.

ARRA has amended HIPAA to specify that the government can now prosecute an employee or another individual for wrongful disclosure if he or she obtains or discloses information maintained by a covered entity without authorization.

In an effort to assist our Business Associates with compliance and understanding of the HIPAA requirements, EBD has stepped up our security audits of State Agencies and Public School Districts. If you have not received a security audit, if it has been awhile since your last audit, or if you would like to be scheduled for a security audit, please contact us at EBDSecurity@dfa.arkansas.gov

Another important change that will be effective soon under the HIPAA portion of the ARRA law, also known as the "HITECH Act of 2009", is the new rules for breach notification. Under the HITECH Act, a breach is considered to have occurred when an individual's unsecured data is compromised. It is very important that as a Business Associate of the Employee Benefits Division, that you notify EBD within 24 hours if you suspect that any member of this Plan's data has been compromised in any way.

If you have any questions about the privacy or security regulations, your responsibilities as a Business Associate, or if you would like to request additional HIPAA training, please contact EBD Security.

Thank you,

Amy C. Tustison
Compliance Officer