

HRconnection®

Security Information

HRconnection® helps you manage company information in one secure and convenient location that employees can view from any computer with Internet access. It lets employers provide its employees with a comprehensive resource for company and benefits information.

Since HRconnection may contain salary information, social security numbers, and employee benefit election information, the existing security safeguards were reviewed to insure compliance with the HIPAA Security Regulations.

While the information contained within HRconnection is sensitive, arguably it does not constitute ePHI when it is created by the employer. Rather, this information is enrollment data that constitutes an "employment record" as described within the HIPAA Privacy Regulations. While we concluded that the information within HRconnection is not ePHI, the security safeguards applicable to HRconnection have been enhanced to comply with the requirements contained within the HIPAA Security Regulations.

- **Storage of Data & Access Control.** Information contained within HRconnection is currently stored in a manner which complies with the HIPAA Security Rules. For example, a disaster recovery plan is in place that allows HRconnection to protect against a loss of data in the event of an emergency, including fire, system failure, or natural disasters. All data entered into HRconnection is stored on servers protected by firewalls and intrusion detection systems. All users are provided with a unique user identification. Access to ePHI within HRconnection is limited to individuals with a need to know.
- **Security Incident Reports.** Security Incident Reports are made available electronically within HRconnection's administration page. A Security Incident means an attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.
- **Automatic Logoff.** A modal window¹ feature is in place that locks out the HRconnection site if it remains open but inactive for 30 minutes. The modal window prevents unauthorized users from viewing or accessing the site. If the user enters his or her password, he or she will be returned to the screen last visited.

Be assured that [b_officialname] understands the importance of the protections afforded individuals by the HIPAA Security Regulations, and that information stored within HRconnection is secure.

Please feel free to contact your Brown & Brown Consulting representative with any questions.

HIPAA Security Regulations

In February 2003, the Department of Health and Human Services (HHS) released final HIPAA Security Regulations. These regulations require that basic safeguards be implemented to protect Electronic Protected Health Information (ePHI) from unauthorized access, alteration, deletion, or transmission.

Health plans, health care clearinghouses, and health care providers that conduct certain transactions electronically ("Covered Entities"), are required to comply with the regulations no later than **April 20, 2005**. Small health plans have an additional year to comply.

Business Associates are required to comply with the HIPAA Security Rules because they use, disclose, or create ePHI on behalf of these entities.

This article is intended to briefly explain how HRconnection® has been enhanced in light of the requirements contained within the HIPAA Security Rules.

¹The modal window lock out feature only applies to HRconnection sites that have the ability to hold salary information.