



Risk of Employee Access to Patient Information and Red Flags Rule Compliance

By Mo Syed, King & Ballow Attorney & Healthcare Practice Member

msyed@kingballow.com

Health care providers are increasingly discovering that information technology is a double edged sword, providing great benefits, but also raising the potential for violations of privacy and identity theft by their own employees. All providers must assess the risk of identity theft posed by their use of information technology by November 1, 2009, when the Federal Trade Commission's Red Flags Rule (RFR) goes into effect.

Employee misuse and unauthorized access to patient information has been a growing concern. A recent case in California typifies this concern. A health care provider who operated a residential care facility providing treatment to patients with drug addictions discovered a former employee allegedly stole sensitive patient information to use in his own competing business. This case involved facts that arose prior to the RFR going in to effect and centered upon the damage to the provider as a result of the employee's actions. However, it illustrates a potential risk for identity theft triggering compliance with the RFR. After the RFR takes effect on November 1st, providers must ensure they comply with their obligations to protect against unauthorized access to information which can be used for identity theft.

The California case is just one example of instances in which employees can gain access to patient information for unauthorized purposes. The potential for employee access to patient information poses important obligations upon providers to



comply with RFR. The RFR applies to information related to patient's identity including, but not limited to medical identification numbers, social security numbers, drivers license numbers, credit card information, insurance claim information, business identification numbers, employer identification numbers, personal health information, and other types of information related to patient identity.

Failure to adhere to the RFR can subject providers to civil fines as well as damaging the reputation of their practice and other adverse consequences. The FTC is authorized to bring enforcement actions in federal court for violations, and could enact penalties of up to \$3,500 per violation of the Rules. The RFR also authorizes states to bring actions on behalf of their residents and each consumer (patient) may be entitled to recover actual damages sustained from a violation.

As we have advised in our prior posts (see the links and listings below), the RFR requires health care providers (among other businesses) to follow four basic steps: (1) identify ways in which identify theft could possibly occur; (2) create policies and procedures to prevent such theft; (3) educate employees; (4) maintain vigilance to detect theft and potentials for theft.

The RFR imposes an obligation to assess risks of identity theft posed by employee access to identity related information. In the context of health care providers, such information may be found accounting records, patient electronic medical records, computer files, and other places where information might be stored. The risks are likely greater when employees are able to email such information to their home computers, as well as access information offsite on computers that are not within the provider's secure network. Employers should be especially vigilant



against permitting employees to utilize thumb drives, iPods and other devices which allow such information to be stored and transferred.

Under the RFR, a provider has an obligation to assess risks of identity theft in its information management systems. It must determine whether additional risks of identify theft are created by allowing employees to either send information to private email accounts, or access company networks from home computers. Below are some issues providers should consider and address:

- Are employees permitted to transfer information to home or other remote locations? If so, what measures are taken to limit or monitor such transfers?
- Are providers educating employees in identity theft risks and restricting access, where feasible, only to information that does not involve identify theft risk?
- Are accounts of former employees promptly terminated and their passwords deleted? (Policy prohibiting post-termination use of computers/passwords should be clearly communicated to all employees.)
- What procedures are in place to prevent unauthorized access via thumb drives and iPods or other information storage devices?
- Are employees required to keep their passwords secure, to change them on a regular basis, and to create passwords with uncommon characters and patterns?
- Are mechanisms in place to detect unauthorized access by former employees and others?
- Have employees been advised to notify providers of any account IDs and passwords they are using? (Are there procedures when employees leave or change jobs within the practice to ensure all passwords/user IDs are identified and access to accounts is terminated as appropriate?)
- Have procedures been established to address action to follow when a breach is identified?



Employee access of sensitive information creates risk of identify theft and therefore, the implications must be carefully addressed. Contact me if you would like to know more about Red Flags Rule requirements and compliance.

To access our prior posts on the Red Flags Rule, click these posts below:

[“FTC Delays Red Flags Implementation,” August 4, 2009](#)

[“Red Flags Rule for Healthcare Providers,” July 30, 2009](#)

For more information contact: Mo Syed, Attorney & Health Care Practice Member at King & Ballow, msyed@kingballow.com, phone (615) 726-5418.

For more posts of interest to health care professionals go to:
www.kingballow.com/healthcare.php

These opinions and comments are intended only for the purpose of providing recent updates and general information and are not intended, and should not be used, as a recommendation for any specific situation or entity or as a substitute for legal counsel. Always consult with an attorney for specific legal counsel concerning your particular situation.