

RED FLAGS RULES ANSWERS

IMPORTANT NOTE – Selarity developed the Red Flags Solutions to bring us and other small businesses into compliance with the Red Flags Rules. We are committed to sharing accurate information but our opinions of the facts regarding the Red Flags Rules are not legal opinions. We are not offering legal advice. It is not possible for us (or anyone) to guarantee that any program will place an organization in compliance with state or federal laws or regulations, as events, circumstances and applicability continually change.

Q. Who must comply with the Rules?

Any organization (including not-for-profits) that collects, stores or shares non-public information (such as Social Security numbers, banking information or credit applications) or run credit or background checks or handle debt collection, must comply with the Rules. The Rules define those organizations as Creditors.

Q. What is the definition of a Creditor?

Any entity that regularly extends (offers), renews, or continues credit, regularly arranges for the extension, renewal, or continuation of credit, or any assignee of an original creditor who is involved in the decision to extend, renew, or continue credit is a creditor.

Most insurance reimbursed services cause the provider of those services to fall under the definition of a creditor. Collection of copayments and deductibles, and then deferring payment for the remaining balance until reimbursed by a third-party, is by definition, extending credit.

It's less likely that the rules would apply if all payments are collected up front. The rules also don't apply if payment is cash or credit cards, because that's not deferred payment. However, routine practices such as setting up a payment plan or billing a third-party mean that the Rules do apply.

Q. What must an organization do to comply with the Rule?

Think of best business practices. Compliance with the Rules means developing a written document that thoroughly details the measures your organization will take to protect the personal identifying information of both its employees and consumer clients. There are specific components that are mandated in the Rules, and for a Program to be complete, all elements must be contained in a Program.

A written plan is worthless unless all of the staff understand and implement the plan into their daily activities. Therefore, all staff must

be trained and required to then sign documents that confirm they have been trained. Then, inspect what you expect!

All vendors and service providers who have physical or electronic access to sensitive information (accountants, cleaning services, data management services, employment screening services, insurance agents, and temporary staffing agencies) should be notified that they must also comply with the Rules. If compliance cannot be verified, the relationship between organizations must be severed.

Q. What if an organization chooses to do nothing?

No, the FTC's not likely to come knocking on your door to take anyone to jail or impose fines. In fact, very little is likely to happen . . . unless an identity theft incident occurs. As the FTC investigates that incident it is too late to develop and implement a program, and there will likely be liability to law suits in addition to government sanctions.

If an incident occurs and the FTC's investigation reveals an organization did not act reasonably to prevent the identity theft, than there may have been a violation of federal law. That violation may subject the organization as well as officers of that organization to civil liability, business-to-business liability, government civil liability, and state and federal liability suits. Fines may be involved. Some of the damages may be irreparable.

While there may be a shared belief that because the FTC will never make it across the threshold of a business, it's probably a safe bet that an eager attorney will find the one's who do nothing. If hit with an unfair business practices suit, a corporation shell might not shield officers from an aggressive probe. In other words, every affected organization probably needs to be in compliance to protect themselves, their employees, other businesses and consumers.

Q. If an organization is in compliance with the Health Insurance Portability and Accountability Act (HIPAA) security rules, isn't that enough?

There is a great deal of overlap between the processes of HIPAA and the Red Flags Rules, but they are independent programs that need to stand alone. HIPAA is primarily controlling access to information. The Red Flags Rules focus on verifying identity of the individual who is the consumer.
