

## **Red Flags Policy Assessment**

### **Implementing a Non-Public Information (NPI) policy regarding data security and "Red Flags"**

An NPI policy, complete with "Red Flags" should be incorporated into your procedural file.

Use the below guidelines and action items as your Checklist to help guide you through the process.

**\*\*BE SURE TO HAVE YOUR ATTORNEY REVIEW YOUR POLICY\*\***

[www.NARPMpartner.com](http://www.NARPMpartner.com)

#### **1- What policies do you have in place right now?**

- i. Review your current policies with staff by department to identify potential risks.
- ii. Are the policies being implemented?
- iii. Do the policies fit the current work environment?
- iv. Review Templates for ideas to incorporate into your office policy.
  1. We will provide you with a few [Email Vicky@VickyMethven.com to be invited to the DropBox](mailto:Vicky@VickyMethven.com)
  2. Jean Storms <http://www.landlordsource.com> also has PM templates to purchase if you choose.

#### **2- Who has access to Non Public Information "NPI" at your office?**

- i. Where is your fax machine?
- ii. Do you have email security?
- iii. Do clients have access beyond your Front Counter?
- iv. What is your Shredding Policy?
- v. Do you have a Janitorial Service?
- vi. Is your building alarmed?
- vii. What is your policy regarding employees who leave your company?
- viii. How often do you change passwords?
- ix. Do you have a "Clean Desk Policy"?

#### **3- Credit Reports & Background Checks?**

- i. What information is your office receiving?
- ii. Where is this information stored?
  1. Accepted Tenants?
  2. Past Tenants?
  3. Rejected Tenants?

#### **4- How is information transmitted to vendors?**

- i. Secure websites? Fax? Email?

#### **5- How is information stored in your office?**

- i. During application process?
- ii. After move in?
- iii. Declined Tenants?

#### **6- How is tenant information safeguarded by Vendors?**

- i. What safeguards do your 3<sup>rd</sup> party vendors have in place to protect your tenants?
- ii. Site Vendors – do they have a Red Flags Policy?
- iii. Do you have it on file?

#### **7- Have you Appointed a Compliance Security Office for "NPI"**

- i. Regardless of whom you have designated as the Chief Information Officer prior, the new laws ask that you also appoint that individual as the new NPI security officer.

#### **8- Train and educate all employees on ID Theft, the new NPI Policy, and "Red Flags"**

- i. Include an acknowledgement form to document employee attendance for personnel file)
- ii. Every compliance program becomes stronger when the employees become aware of their responsibilities when handling consumer, vendor, or employee information.

#### **9- Install an ID Theft Monitoring/Restoration/Legal Service program for all employees as an optional voluntary payroll deduction benefit, subsidized benefit, or fringe benefit.**

- i. (Opt in /opt out required)
- ii. This benefit provides a mitigation plan and early warning system that allows the employees the option to protect their families from these growing concerns.
- iii.

#### **10- Provide 3<sup>rd</sup> Party Vendor Letters**

- i. New laws call for 3<sup>rd</sup> parties to be required to protect client/employee NPI just as you have.
- ii. Be sure to obtain copies of their Red Flags policies as well.

[See the FTC template for low risk businesses.... This is a basic place to start.... we will assist your vendors. Please Call.](#)