

(SAMPLE) CHECKLIST FOR RED FLAGS PROTOCOLS

- Incorporate Data Security safeguards:**
 - Physical security
 - Network security
 - Personal computer security
 - Remote access security
 - Offsite data security

- Implement protocols to check for signs of potential credit or personal information theft or use of “stolen” identity:**
 - Limit programs that may be downloaded to office computers
 - Use applicable filters to prevent potential spam that may contain phishing attempts, or the inadvertent downloading of “malware” that may steal sensitive information
 - Carefully check suspicious documents presented for identification (that may have been altered or forged)
 - Check photographs on identification to ensure it is the person presenting it
 - Check to ensure that information on the identification is consistent with other information presented (address, social security number, etc.)
 - Check carefully on any mail or email that is returned
 - Beware of P.O. boxes used for addresses

If your system holding personal data has been compromised, do the following:

- Notify Law Enforcement**
 - Call local police department immediately
 - If local police are not familiar with investigation information compromises, contact the local office of the FBI or U.S. Secret Service
 - For incidents involving mail theft, contact the U.S. Postal Inspection Service.

- Notify Affected Businesses**
 - For a theft of account access information (e.g., credit card or bank account numbers), notify the institution that maintains the accounts to allow them to monitor the accounts for fraudulent activity
 - For theft of Social Security Numbers, contact the major credit bureaus for additional information or advice. This will facilitate customer service if your patients request fraud alerts for their files.

Equifax
U.S. Customer Services
Equifax Information Services, LLC
Phone 1-800-685-1111
Email: businessrecordsecurity@equifax.com

Experian
Experian Security Assistance
PO Box 72
Allen, TX 75013
Email: BusinessRecordsVictimAssistance@experian.com
Phone: 888-397-372

TransUnion
Phone: 800-372-8391

Notify Individuals

- Early notification to individuals whose personal information has been compromised allows them to take steps to mitigate the misuse of their information. When deciding if notification is warranted, consider the nature of the compromise, the type of information taken, the likelihood of misuse, and the potential damage arising from misuse. Individuals who are notified early can take some steps to prevent or limit harm if names and Social Security numbers have been stolen.
- Consult with law enforcement about the timing of the notification so it doesn't impede their investigation
- Designate a contact person within your practice who can release information, and keep that person up to date with the information on the breach, your response, and how individuals should respond.