****

#3 Information and Data Privacy  
Adopt and maintain a written privacy and information security program to protect Non-public Personal Information as required by local, state and federal law.

|  |  |  |
| --- | --- | --- |
| Purpose Federal and state laws (including the Gramm-Leach-Bliley Act) require title companies to develop a written information security program that describes the procedures they employ to protect Non-public Personal Information. The program must be appropriate to the Company’s size and complexity, the nature and scope of the Company’s activities, and the sensitivity of the customer information the Company handles. A Company evaluates and adjusts its program in light of relevant circumstances, including changes in the Company’s business or operations, or the results of security testing and monitoring. | | |
| What You Should Know An attorney is required to protect the confidentiality of all client matters, including information in paper and electronic media. Rule 1.6, Confidentiality of Information, of the Revised Rules of Professional Conduct.  The Federal Trade Commission defines NPI as:   * any information an individual gives you to get a financial product or service (for example, name, address, income, Social Security number, or other information on an application); * any information you get about an individual from a transaction involving your financial product(s) or service(s) (for example, the fact that an individual is your consumer or customer, account numbers, payment history, loan or deposit balances, and credit or debit card purchases); or * any information you get about an individual in connection with providing a financial product or service (for example, information from court records or from a consumer report).   Examples of NPI include:   * bank, loan payoff and credit card statements; * insurance, retirement and tax information; * Social Security numbers and dates of birth; and * real estate/title related items, commission amounts and loan fees.   There are many sources within a company where NPI can be found. Physical locations such as paper-based files, desktop or reception area, the closing table and warehouse. With the widespread use of smart phones, be vigilant of the documents visible to anyone other than vetted employees, such as at the closing table.  There are also many electronic locations where NPI is housed. These include:   * Computers, laptops, ipads, flash/thumb drives, network servers, email servers, instant messaging servers, fax servers, copy machines with internal hard drives or network storage devices, web servers, etc. * Cloud storage (e.g., Google, Dropbox) * Backup tapes; online backup services * User-provided devices/media (e.g., smart phones, tablets, USB storage devices)   Additionally, NPI can be found and in possession of vendors a company may utilize. These include notaries, couriers, online backup services or off-site backup tape storage vendors, email service providers, and server and website hosts. Take reasonable steps to select and retain service providers that are capable of appropriately safeguarding NPI. |  | Issues to Consider and Discuss  * Is your entrance separated from your closing rooms and workspaces by a door, a receptionist or some other form of protection? * Where is your server located? Is it isolated in a locked closet, room or other area with limited access? * Who has access to the areas that have private/confidential information? Consider cleaning services, repair technicians, realtors, other clients and other third parties. Do vendors, such as janitorial services, water and coffee suppliers, etc. have access to areas that have private/confidential information in use? * Do you have a “clean desk” policy? * Do you have a proprietary email address? Do you assure *no one* in your firm shares client NPI on a public network such as using their private gmail, hotmail, yahoo or AOL email? * Do you meet with clients in a conference room rather than your office? Are other clients’ matters visible? Do other parties have access to a closing file if you leave the room? * Could an employee or others upload or download data using a portable memory device? * How do you dispose of paper records? * What would happen in the event of a natural disaster – flood, hurricane or accidental disaster (power outage, sinkhole, fire, vehicle impact to building)? * What does your current insurance cover in the event of a disaster? Research various insurance coverages available. Do you need to adjust your coverage?  Ethics opinionsRule 1.16, Confidentiality of Information, Revised Rules of Professional Conduct, Reasonable precautions and expectation of privacy, Comment 18Using outside software vendors, including banks, 2011 FEO 6 and 2011 FEO 7Recycling, RPC133Disposal of client files, RPC 209Email, RPC215, 2009 FEO 1Cellphone, RPC 215Website /internet storage, 2008 FEO 5Software as a service 2011 FEO 6 |