Tips for brokers to consider when creating a Written Information Security Plan ("WISP")

When determining whether or not your office falls with the scope of the new regulations, the threshold question to consider is whether or not you maintain or store personal information of a resident of the Commonwealth. This can include, for example, a client, customer, employee or agent affiliated with your office.

Some of the common areas where REALTORS® often collect personal information include:

1. **Rentals**- Rental applications typically require a prospective tenant's social security number for the purposes of running credit checks. If the application is in hardcopy, as most are, be sure, for example, to keep that document in a locked file cabinet or redact any social security number or other personal information.
   SAMPLE WISP LANGUAGE: "*Files with hard copy rental applications containing personal information will be kept in a locked file cabinet when not in use by the agent"* or *"personal information contained on a rental application will be redacted before being placed in the file."*

2. **Short Sales**- It is not uncommon for listing brokers to have personal information (financial account numbers or social security numbers) when working with a seller facing a short sale, particularly if the REALTOR® is working directly with a lender on the seller's behalf. Various documents in the file many contain personal information. Keep the file secure when not in use and ensure that only the necessary personnel have access to the file.
   SAMPLE WISP LANGUAGE: *"Files containing any hard copy documents with personal information shall be secured in a locked file cabinet (or locked office, or desk drawer, etc.) when not in use."*

3. **Check Deposits**- When acting as escrow agent on a transaction, personal checks are commonly provided as a good faith deposit. If the check contains a bank account number and a copy of the check is kept on file, then personal information is being stored.
   SAMPLE WISP LANGUAGE: "*Copies of all good faith deposit checks shall be kept on file. If copies contain a personal bank account number, such information shall be redacted. Copies of checks shall not be kept in an electronic manner."*

4. **Interest Bearing Escrow Accounts**- Whether or not funds should be deposited in an interest bearing account depends on agreement between the parties and the willingness of the escrow agent to assume the significant accounting responsibilities that come with maintaining an interest bearing account. Review your escrow clauses in your forms. Non-interest bearing accounts will eliminate the requirement of using IRS forms such as the 1099 or W-9 which may require you to collect and maintain personal information.
   SAMPLE WISP LANGUAGE: *"It is the policy of this office to maintain a non-interest bearing escrow account. If parties choose to keep funds in an interest bearing escrow account during the pendency of transaction, then such funds shall be held by a third party mutually agreeable to the parties."*

5. **Other Personal information** – Information which may be contained in files of brokers and salespersons affiliated with the firm and any employees.
   SAMPLE WISP LANGUAGE: "*Files containing personal information shall be restricted and maintained in a locked file cabinet at all times."*

Areas to examine in developing your WISP:

- **Type of office and services provided.** No two real estate firms are alike. Offices range in size from small single broker officers to large offices with dozens of agents with multiple office locations. The type of services offices offer to clients and customers varies as well- rentals, residential, commercial, industrial, etc. Agency relationships can differ from single agency to dual agency, designated agency or non-agency facilitator relationships. Standard forms vary depending on the source. Record retention policies, storage space, and computer networks differ within offices. Because each office is different, each office must develop its own written WISP based on its own practices and procedures.

- **Review and determine what personal information you have on file and regularly use in transactions.** It is always a good idea to check your office policies and practices, including the forms used for transactions, to determine if there is any unnecessary personal information being collected. If you find instances where personal information is being collected without a specific need, consider changing your office policy to stop gathering that information. For example, there is typically never a reason to have any social security number on a purchase and sales agreement. Consider instructing clients and customers not to complete this information or line through the text.

- **Ongoing or current transactions**. If a file contains personal information of clients and customers, reasonable steps should be taken to ensure that the information remains secure. In many transactions there won't be a need to collect any personal information. In those instances where personal information is necessary, reasonable steps should be taken to keep that information secure. These steps will vary under the circumstances but can include for example, keeping files in secure or locked desks or filing cabinets, redacting personal information from files, or shredding those documents with personal information if they are no longer necessary. A WISP should indentify who will have access to those files containing personal information and limit such access to include only those with a legitimate business reason. Consider indentifying such files as "confidential."

  SAMPLE WISP LANGUAGE: *"Access to records containing Personal Information shall be limited to those individuals who are reasonably required to know such information in order to accomplish the legitimate business purpose. Agents shall not keep open files containing Personal Information on their desks when they are not at their desks."*

- **Visitors**. When a visitor (including customers, clients, colleagues, delivery personnel, cleaners, etc) enters your office, consider how to restrict them from accessing electronic or hard copy personal information. For larger offices, this might include, for example, a means to have visitors sign-in and/or wear name badges. If you have a wireless network in your office, ensure that visitors cannot access your network. In all cases, the standard is to take reasonable care to protect the sensitive information.
  SAMPLE WISP LANGUAGE: *"Office visitors (including customers, clients, colleagues, delivery personnel, cleaners, friends etc) shall sign in at the registration desk and/or wear name badge. Employees will take reasonable steps to restrict visitors from accessing personal information or non-public sections of the network."*

- **Encryption**. The regulations also require encryption of personal data when it is stored or transmitted electronically where technically feasible. The WISP should identify what personal information, if any, will be stored or transmitted electronically and what steps will be taken to ensure security. The regulations require encryption of personal information in all electronic forms only if technically feasible. This means that reasonable efforts should be used to encrypt. Encryption is the process of converting data into a format that cannot be read by others. Certain software such as Windows XP or Windows 7 has the ability to automatically encrypt your data. If your software does not contain such features, consider consulting an IT professional or purchasing encryption software.

  SAMPLE WISP LANGUAGE: "*Agents maintain portable electronic smart phones and laptops. To the extent technically feasible, all Personal Information stored on laptops or other portable devices shall be encrypted as well as all records and files transmitted across public networks or wirelessly, to the extent technically feasible.*"

- **Passwords and Computer Security**. All employees and agents should have an individual password to access their computer. Unique passwords which are difficult to guess reduce the risk of unwarranted access to your network. Consider requiring that all passwords be changed periodically (every several months) for security purposes. Firewalls, virus protection, spyware and malware protection software are all good tools to prevent unauthorized access. These should be updated on a regular basis. Access to the network should be terminated when an employee or agent leaves the firm by eliminating the user's account and password.

  SAMPLE WISP LANGUAGE: "*Access to electronically stored Personal Information shall be electronically limited to those individuals having a unique log-in ID; and re-log-in shall be required when a computer has been inactive for more than a few minutes. When an agent disaffiliates with this office, physical and electronic access to Personal Information shall be immediately blocked. Such agents shall be required to surrender all keys to this office. Moreover, such individual's remote electronic access to Personal Information shall be disabled; his/her voicemail access, e-mail access, internet access, and passwords shall be invalidated."*

- **Closed files and record retention.** The WISP should identify a procedure to reasonably secure files for past transactions if they contain personal information. Offices should retain records in the most economical and practical method and location, including offsite storage when appropriate. For example, if your office storage space is too small or does not have sufficient locked storage, consider moving older files to an offsite location. When not being used by authorized personnel, or when not clearly visible in an area where authorized persons are working, all hardcopy personal information should be secured, for example, by locking in a file cabinet, desk, safe, storage area, or other furniture. Likewise, when not being used, or when not in a clearly visible and attended area, all computer storage media (thumb drives, tapes, CD-ROMs, etc.) containing personal information should be locked in similar enclosures.

  Each office should develop a record retention policy. A rough rule of thumb is that records should be kept at least seven years, since the statute of limitations for a claim for breach of contract is six years. Certain documents, such as corporate records, partnership agreements, audit reports, general ledgers, tax returns and deeds should be kept permanently. When agents leave a firm, all files should be turned over to the office (unless otherwise agreed). Check with your attorney/accountant to develop a specific written record retention policy.

- **Home offices.** If agents are working from a home office, they should maintain the same level of care in protecting personal information. A WISP should address this and identify whether or not, for example, the broker reserves the right to grant and revoke telecommuting rights or the opportunity to inspect (during normal business hours) the home office to ensure compliance. Telecommuting may be granted based on communications, physical and information security capabilities.

  Since REALTORS® frequently have customers and clients in their automobile if any documents or files containing personal information are left in a car, care should be utilized so that passengers cannot readily access such information.

  SAMPLE WISP LANGUAGE: "*Agents will use caution when keeping personal information in their automobile. Such information shall be stored in a secure manner such that passengers cannot readily view any personal information. Automobiles shall remain locked at all times when personal information is left unattended*."

- **Third Party Vendors.** Vendors who have access to your network and personal information stored on the network, reasonable and diligent efforts should be used to determine if the vendor is capable of maintaining procedures to keep information secure consistent with the Regulations. This can be done, among other ways, by asking for a notice that the vender is in fact compliant with these regulations. If there is a contract with the vendor, it should include a provision that requires compliance (see 201 CMR 17.03(2)(f)).

- **Compliance**. All employees and independent contractors affiliated with the firm should be notified of the WISP, acknowledge receipt, and ensure their compliance with the polices of the office. Training and instruction on the WISP and related matters should be conducted periodically. An annual review and update of the WISP is another good way to ensure ongoing compliance with the Regulations. Any incidents where a breach of security has occurred and personal information has been compromised, a WISP should set forth a procedure for reviewing office procedures and implement changes if necessary.

  SAMPLE WISP LANGUAGE: "*All security measures shall be reviewed at least annually, or whenever there is a material change in business practices occurs that may reasonably implicate the security or integrity of records containing Personal Information. The Data Security Coordinator shall be responsible for this review and shall fully apprise the Broker of Record of the results of that review and any recommendations for improved security arising out of that review.*"