ALTA Best Practice #3: A Primer on How to "Think About" Information Security & Privacy

Overview

The intent of this document is to stimulate thinking and questions about information security related to Pillar 3 of the American Land Title Association's (ALTA) Best Practices for Title Insurance and Settlement Companies. Securing information is challenging due to the incredibly wide variety of ways in which information is accessed, used, changed, stored, shared and destroyed. By their very nature, many business operations rely solely on the processing of information for the creation of value. As such, many systems today are not designed around complex security requirements but are instead geared toward ease of use and information sharing.

In spite of the above, many laws and regulations demand information governance and controls to minimize the risk of loss of nonpublic personal information (NPI). All applicable federal laws and regulations are designed around a general notion of "reasonableness," and we will develop herein a method to address that principle. To understand the challenge of assuring information security, we'll begin by first outlining the regulatory environment and a general methodology for addressing the regulatory requirements. We then describe the nature of NPI and a way to consider the complexity of business operations with respect to requirements to protect NPI. With this understanding of the complexity, we will then look at various dimensions of security that must be considered regardless of the complexity of the business.

Laws and Regulations

GLBA: The Gramm-Leach-Bliley Act (GLBA) was enacted in 1999. The Federal Trade Commission (FTC) and state departments of insurance generally adhere to July 1, 2001 as the act's effective date. The FTC, along with other federal regulators, and most state insurance regulators, adopted regulations to clarify privacy obligations under the act.[1]

- GLBA protects the NPI of individual consumers engaged in non-commercial transactions. It does not protect the NPI of businesses engaged in commercial transactions. The act regulates financial institutions defined as:

> "Any institution, the business of which is engaging in activities that are financial in nature or incidental to such financial activities, as determined by Section 4(k) of the Bank Holding Company Act of 1956. Financial institutions can include banks, securities brokers and dealers, insurance underwriters and agents, finance companies, mortgage bankers, and travel agents."

[1] For additional FTC information on GLBA compliance, see: https://www.ftc.gov/tips-advice/business-center/guidance/how-comply-privacy-consumer-financial-information-rule-gramm

- In addition, the FTC includes, in the definition of financial institutions, anyone who performs *settlement services* involving the sale, purchase, or finance of an individual's home – including those who provide the following products and services:

Closings	*Escrow*	*Surveys*
Appraisals	*Flood Certifications*	*Exchange Services*
Tax searches	*Title searches*	*Title insurance policies*
Credit reports	*Notary services*	*Document preparation*

Methodology

Based on our interpretation of the law and regulations, an Agent must fundamentally consider the following five-part question:

What NPI do we handle, who can access it, what methods are used to access and share it, how is it destroyed, and finally how are we minimizing the risk of loss of that information?

Once this multi-part question is answered, an Agent must develop and capture the following:

- Policies that outline the intent to protect and minimize the risk of loss of NPI.
- Procedures that, if followed, would reasonably protect and minimize the risk of loss of NPI.
- Within the organization's policies and procedures, provisions regarding training for employees and other third parties that have access to the NPI.
- Evidence that the procedures are being followed over time.

Nonpublic Personal Information (NPI)

In order to address the requirements of the existing federal regulations and bulletins, an organization must first determine the type and form of the NPI that it handles. NPI generally is any information that is not publicly available and that:

- A consumer provides to a financial institution to obtain a financial product or service from the institution;
- Results from a transaction between the consumer and the institution involving a financial product or service; or
- A financial institution otherwise obtains about a consumer in connection with providing a financial product or service.

Nonpublic personal information may include individual pieces of information as well as lists of information. For example, NPI may include names, addresses, phone numbers, social security numbers, income, credit score and information obtained through Internet collection devices (i.e., cookies).

Once an organization understands the type and form of NPI it handles, its next step is to understand the complexity of its operations as related to handling NPI.

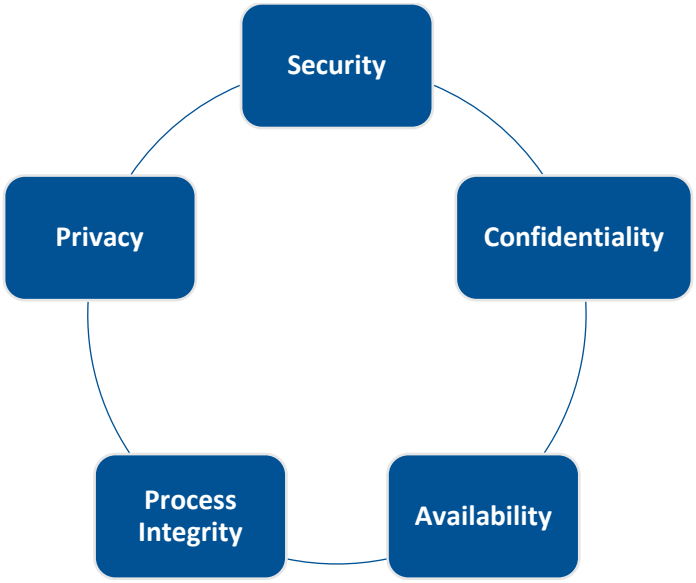
Organizational Complexity

It is only with an understanding of its complexity that an organization can be confident in responding to the question of reasonable controls over NPI. For Agents, the following matrix lists a number of areas that should be considered to understand and be able to explain to lenders and regulators the nature of the risk of loss of NPI handled by the organization.

Measure of Complexity	Considerations
Transaction Volume and Value	Degree of automation; # of hand-offs
Number of people	Division of responsibilities
Number of locations	• Connectivity • Offices / Homes / File storage
Mechanisms for NPI access	
Paper files	Clean desk / Workspace
Hardware number, type, versions	• Desktop / Laptop • Tablet / Phone
Software versions	• Off-the-shelf application(s) • Custom application(s)
Mechanisms for NPI storage	
Paper files	Basic lock & key
Software Application	Passwords
Network shared files / Cloud	Service Level Agreement
Mechanisms for NPI distribution	
Paper files	Restrict to “need to know”
Software Application	Restrict to those with valid business need
Copies	• Network shared files • Email • Phone / Fax / Texting • Cloud • Physical transport / USPS / FedEx / UPS
Outsourced Transaction Services	
Searching/ Notary /Closing / Recording /Policy Production / Bank account reconciliations / Document scanning and imaging	Contract with only reputable and qualified service provider(s) in order to contain operational, reputation and regulation risks. When you outsource it does not diminish nor absolve you of being primarily responsible – the lenders hold YOU responsible to oversee and manage the outsourcing.
Technology Services	
Equipment management	• On-site • Co-location hosting / Cloud • Virtual or physical • Anti-virus / Anti-malware
Network Infrastructure management	Office / Home
Software Application Administration	Monitor, Review, Approve
Disaster Management / Recovery	Set timeframe in contract, and test it
Backup & Restore	Off-site storage

Considerations

The next step is to consider the various aspects of complexity along five dimensions: Security, Privacy, Confidentiality, Availability, and Process Integrity. These dimensions are designed to help assess the ultimate risk of loss of NPI. Each of these dimensions can be considered using the basic questions of Who, How, Where, What, and When.



For example, when thinking about the areas outlined in the previous section, the idea of "Backup & Restore" should be considered relative to security, confidentiality, availability, privacy and process integrity. This means that one needs to consider the following types of questions:

1. How and when are backups performed? (Process Integrity)
2. Where is the backup media stored? (Privacy, Security)
3. Who has access permissions to perform, review and maintain the backups? (Privacy/Confidentiality)
4. Who ensures the backups are successful? How? (Availability, Process Integrity)
5. Who performs periodic restores to verify the quality of the backups? (Process Integrity)
6. When are backups destroyed? (Confidentiality)
7. How long will it take before my data is restored and I'm back in business? (Availability, Process Integrity)

Policies

Policies should be simple, direct, written text explaining what is done and what it covers. The following examples are suggested starting points for your policies:

Example 1: "Information Security" policy

> *This policy establishes company-wide strategies and responsibilities for protecting the confidentiality, integrity, and availability of the information assets that are accessed, managed, and/or controlled by the company. Information assets addressed by the policy include data, information systems, computers, network devices, as well as documents and verbally communicated information.*

(Note: The information security policy language should also include a notion of compliance with federal consumer protection laws such as GLBA).

APPROACH

Your policy should set forth an effective information security framework to appropriately secure access to information resources and services. The policy should address:

- How to protect against unauthorized access to, use, or sharing of, sensitive information that could potentially result in harm to the company or to members of the company's community;
- How to protect against anticipated threats or hazards to the security of information assets;
- How to comply with federal, state, and local law, company policies, and agreements binding the company that require the company to implement applicable security safeguards;
- How to recognize risks or threats; and
- How to handle a breach or loss of NPI or sensitive data.

The information security policy should include the following tenets:

- Members of the company have individual and shared responsibilities to protect the information assets controlled by the company in accordance with federal, state, and local law, company policies, and agreements binding the company.
- The company will develop, maintain, and implement an information security plan which will define security initiatives.
- The company will identify and track sensitive and critical Information assets under its control. Information assets will be classified relative to the level of risk that their compromise may pose to the institution.
- The company will periodically conduct risk assessments around its sensitive and critical information assets. Risk assessments will prioritize risks and recommend appropriate mitigation strategies.

Example 2: Privacy Policy

We respect the privacy of our customers' personal information, so we want you to know the ways in which we may collect and use nonpublic personal information. Our practices and policies are set out in this notice.

Types of Information We May Collect:

In the course of our business, the types of personal information that we may collect about you include:

- *Information we receive from you or your authorized representative on applications and forms, and in other communications to us;*
- *Information about your transactions with us, our affiliated companies, or others; and*
- *Information from consumer or other reporting agencies.*

Use and Disclosure of Information:

- *We use your information to provide the product or service you or your authorized agent have requested of us.*
- *We may disclose information to our affiliated companies and unrelated companies as necessary to service your transaction, to protect against fraudulent or criminal activities, when required to do so by law, and as otherwise permitted by law.*
- *We do not share any personal information we collect from you with unrelated companies for their own use.*

Protection of Your Personal Information:

- *We restrict access to personal information about you to those employees who need to know that information in order to provide products and services to you or for other legitimate business purposes. We maintain physical, electronic and procedural safeguards to protect your personal information from unauthorized access or intrusion.*

Changes: *This notice may be revised in accordance with applicable privacy laws.*

Procedures

Procedures are the activities or steps to implement the written policies. It is important to consider each business process (such as order entry, search, exam, closing, policy production, payment, hire, terminate) where NPI (buyer, seller, employee) is handled. Our recommendation is to describe procedures at a sufficiently high level in order to facilitate reasonable flexibility in the process, yet still ensure the process conforms to the procedure in a manner that minimizes the risk of NPI loss.

When developing procedures, it is important to consider:

- Initial intake or receipt of data
- Processing
- Transmitting
- Storage
- Backup
- Disposal

In addition, consideration should be given toward:

- Risk assessment/identification
- Ongoing monitoring
- Testing
- Understanding/Training and participation by all affected employees
- Reporting data breaches

Audit & Compliance Readiness

At the end of the process of ensuring information security, it is important to be able to "*show you do what you say.*" This is the fundamental objective of any documentation program and will allow you to demonstrate your compliance to various requirements. There are a number of things to consider when preparing for an external assessment, including:

- Ongoing and evolving vigilance and monitoring
- Testing and mitigation
- Quality reviews
- Evidence of training
- Evidence of proper NPI destruction

The attached following checklist will assist you with your data security and privacy readiness. If you are able to answer "yes" to all questions, and substantiate with documentation, you are compliant or well on your way to being compliant to existing and anticipated federal and state regulations.

Requirement	Check for YES	Action to Address if NO
Licensee's written information security program must:		
Protect the security and confidentiality of nonpublic personal information (NPI) and the security of the information system;		
Protect against threats or hazards to the security or integrity of NPI and the information system;		
Protect against unauthorized access to or use of NPI and minimizes likelihood of higher to a consumer;		
Define and periodically reevaluate a schedule for retention of NPI and a mechanism for its destruction when no longer needed;		
Licensee - Insurer and agent/producer - must:		
Designate one or more employees, an affiliate, or an outside vendor to act on behalf of licensee as to responsible for the information security program;		
Identify reasonably foreseeable internal or external threats to the unauthorized access of NPI, including the security of information systems and NPI accessible to or held by third-party service providers;		
Assess the likelihood and potential damage of these threats, considering the sensitivity of the NPI;		
Risk Assessment **Assess the sufficiency of policies, procedures, information systems, and other safeguards in place to manage these threats, taking into consideration threats in each relevant area of the licensee's operations, including:**		
Employee training and management;		
Information systems, including network and software design, and information classification, governance, processing, storage, transmission, and disposal;		
Detecting, preventing, and responding to attacks, intrusions, or other system failures;		
Based on *Risk Assessment* – Licensee must:		
Design the information security program to mitigate identified risks, commensurate with the size and complexity of activities, including use of third-party service providers, and the sensitivity of the NPI;		
Determining & Implementing Security Measures Determine appropriateness of and implement the following security measures:		
Placing access controls on information systems, including controls to authenticate and permit access only to authorized individuals to protect against the unauthorized acquisition of NPI.		

We invite you to visit the Alliant National Agent Resource Center (ARC) for more information and additional resources to assist you with complying with the ALTA Best Practices.