PRIVACY, DATA SECURITY, AND ELECTRONIC TRANSACTIONS – THE EVOLUTION CONTINUES

Rich J. Fidei, Esq., Partner
Colodny, Fass, Talenfeld, Karlinsky & Abate, P.A.

AICP Northwest Chapter 2012 Education Day
Seattle, Washington
May 22, 2012
Disclaimer

The information in this presentation is intended to provide a general overview of the issues contained herein and is not intended, nor should it be construed, to provide specific legal or regulatory guidance or advice. If you have any questions or issues of a specific nature you should consult with appropriate legal or regulatory counsel to review the specific circumstances involved. Transmission or reproduction of any of the information contained herein is prohibited without the express written consent of Colodny, Fass, Talenfeld, Karlinsky & Abate, P.A.
Talking Points

• Privacy
• Data Security
• Electronic Delivery of Insurance Documents
PRIVACY
Privacy

• Gramm Leach Bliley ("GLB") mandates that states enact laws setting forth appropriate standards for protecting nonpublic personal information.

• GLB also provides an insurer’s obligation with respect to disclosures of nonpublic personal information (i.e., privacy policies).
Privacy

• Nonpublic personal financial information:
  • Personally identifiable financial information; and
  • Any list, description or other grouping of consumers (and publicly available information pertaining to them) that is derived using any personally identifiable financial information that is not publicly available.

• Personally identifiable financial information:
  • Provided to a licensee to obtain an insurance product or service from the licensee;
  • About a consumer resulting from a transaction involving insurance product or service between a licensee and a consumer; or
  • Otherwise obtained about a consumer in connection with providing insurance product or service to a consumer.
Privacy

• The Health Insurance Portability and Accountability Act (“HIPAA”) requires covered entities to protect personal health information.

• Governs use and disclosure of individually identifiable health information (i.e., notice of privacy practices).
Privacy

- Nonpublic personal health information:
  - Identifies an individual who is the subject of the information; or
  - Reasonable basis to believe that the information could be used to identify an individual.
Privacy

• A majority of the states require that insurers and licensees implement comprehensive written information security programs.

• Must include administrative, technical, and physical safeguards for the protection of customer information.
Privacy

• Privacy Practices
  • What type of information do you collect?
  • For what purpose do you collect this information?
  • Who will see this information?
  • Will any other companies see this information?
  • What is your affiliation with these companies?
  • Will there be any joint marketing efforts with other companies?
  • Will you use consumer reports, credit scores, or CLUE Reports?
  • If customers request, how can they receive the information you have on file?
  • Use of cookies or other types of data tracking and gathering?
  • Any advertisements on your website for other companies?
Data Security

- Total number of breaches was higher than ever for 2011. *Verizon 2012 Data Breach Investigations Report.*
- The average organizational cost of a data security breach in the U.S. dropped 24 percent to $5.5 million in 2011 from $7.2 million in 2010. *2011 Cost of Data Breach Study, Ponemon Institute, LLC.*
- Health data breaches increased 32 percent from 2010 to 2011 and that the average cost per organization grew 10 percent last year. *Id.*
- In 2011, 95 percent of records lost included personal information, compared with only 1 percent in 2010. *Verizon.*
Data Security

• Almost every state has laws that govern notification of security breaches.
  • Applies to nonpublic personal information (definitions vary by state).
  • Determine whether a breach occurred.
  • Must give notice of a breach within time required.
  • Safe harbor in many states for encrypted data.

• Also, several states have laws that govern the disposal of data.
Data Security

• “Breach” means the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a person or business.

• “Personal information” means an individual’s first name or first initial and his or her last name in combination with one of more of the following, when either the name or the data element is not encrypted or redacted:
  • social security number,
  • driver’s license number,
  • account number with security access code or password, and
  • medical information.
Data Security

- Health Information Technology for Economic and Clinical Health Act ("HITECH") enacted in 2009.
  - Promotes the adoption and meaningful use of health information technology.
  - Strengthens the civil and criminal enforcement of the HIPAA rules.
- Requires health care providers and other HIPAA covered entities to promptly notify affected individuals of a breach, HHS Secretary, and the media in certain cases.
- Annual reporting requirements with HHS.
- Safe harbor for following guidelines to secure information.
Data Security

• What can you do?
  • Strengthen technology to safeguard data.
  • Have a data breach response plan.
  • Right processes and technology to spot a breach.
  • Training.
  • Call the experts.
Data Security

• Data Breach Response Plan
  • Key personnel.
  • Responsibilities.
  • Investigate.
  • What, when, how, who, and where?
  • Stop it.
  • Legal analysis.
  • Update.
Data Security

• “Trade secret” means information, including a formula, pattern, compilation, program, device, method, technique, or process, that:
  • Derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use; and
  • Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

• Other data security implications.
ELECTRONIC DELIVERY OF INSURANCE DOCUMENTS
Electronic Delivery

- In 2000, Congress enacted the Electronic Signatures in Global and National Commerce Act ("ESIGN").
- ESIGN generally provides that a signature, contract, or other record relating to a transaction may not be denied legal effect solely because it is in electronic form.
Electronic Delivery

- State laws and regulations may modify, limit, or supersede ESIGN by:
  - Adopting or enacting the Uniform Electronic Transactions Act ("UETA"), or
  - Enacting laws that are consistent with ESIGN’s principles and technology neutral.
- Every state, except for New York, Illinois, and Washington, have enacted or adopted the UETA in some form.
- The UETA is limited in scope and only applies to electronic records and signatures relating to a “transaction.”
Electronic Delivery

• A *record* or *signature* may not be denied legal effect or enforceability solely because it is in electronic form.

• A *contract* may not be denied legal effect or enforceability solely because an electronic record was used in its formation.

• If a law requires a record to be in *writing*, an electronic record satisfies the law.

• If a law requires a *signature*, an electronic signature satisfies the law.
Electronic Delivery

• Parties have to agree to conduct a transaction by electronic means.
  • Legal document between insurer and insured or potential insured.
  • Consumer may consent to conduct some transactions by electronic means, and not others, or not at all.
  • Critical to define scope of agreement and the types of transactions covered by the agreement.
Electronic Delivery

• If a law requires that information be sent, provided, or delivered in writing, the requirement may be satisfied with an electronic record capable of retention by the recipient at the time of receipt.
Electronic Delivery

- ESIGN consumer protection disclosures:
  - Consent electronically, or confirms consent electronically, in a manner that reasonably demonstrates access to the information in electronic form.
  - Right to receive document in paper format.
  - Right to withdraw consent.
  - Whether consent applies to only the particular transaction or more categories.
  - Procedures to withdraw consent.
  - A statement of the hardware and software requirements for access to and retention of the electronic records.
Electronic Delivery

- Design and implement process.
  - E-mail notifications with link.
  - Secure internet portal.
  - Encryption.
- Mitigate potential risks.
  - Passwords.
  - Time stamps.
  - Identifying information.
  - Prohibit alteration of document.
- Audit and adjust process.
Electronic Delivery

- New York Office of General Counsel 09-01-01 (Jan. 6, 2009)
  - May an insurance policy that has been issued and executed on the Internet be considered a properly delivered and valid insurance contract if the insured prints the policy from the Internet on the insured’s personal computer?
  - Yes. Nothing in the Insurance Law or regulations promulgated thereunder prohibits an insurance company from issuing and delivering an insurance policy to an insured via the Internet if the insured has consented to receiving electronic documents. The electronic documents must conform to applicable substantive and formatting requirements of the Insurance Law and any other applicable laws.
Electronic Delivery

- The UETA is procedural only; underlying substantive state law still governs.
  - If a state insurance law requires documents to be provided by a specific method (e.g., certified or first class mail), this method should be used.
- Some uncertainty as to whether “delivery” as used in the insurance laws would be satisfied by electronic transmission.
- Proof of mailing issues.
Questions?
For More Information

Rich J. Fidei, Esq.
rfidei@cftlaw.com
Direct: (954) 332-1758

South Florida Office
One Financial Plaza, 23rd Floor
100 SE 3rd Avenue
Fort Lauderdale, FL 33394
Main: (954) 492-4010

www.cftlaw.com