

# Protecting Confidentiality in the Face of Regulator Requests



**Presented to AICP, Western Chapter**

**By Elizabeth Tosaris**

**May 6, 2010**

# The Fundamental Issue

---

- Insurers are fearful that regulatory access to confidential communications will result in the loss of confidentiality.
  - Regulatory access to privileged communications will (1) chill the frank exchange of information necessary to attorney-client communications or attorney work product; (2) operate as a waiver of the privilege; and (3) may lead to wrongful or inadvertent release of the information.
  - Production of personal information could lead to exposure to failure to maintain person information in confidence.
  - Providing trade secret information will give competitors an unfair advantage.
- Regulators, on the other hand, worry that licensees may use overstated claims of confidentiality to hide wrongdoing and impede regulators' ability to understand facts fully and to investigate all issues thoroughly.

# Roadmap for Today's Discussion

---

- Types of Confidential Information
- Regulators' Authority to Request Information
- Legal Guidelines
- Best Practices

# Types of Confidential Information

---

Covers a broad range

- Traditional Paper Documents
- Emails and Voice Mails
- Electronic Documents
- Systems and Programs
- Electronic Data
- Other Information

# What is Confidential?

---

- Privileged Information
- Personal Information
- Proprietary Information

# Keeping it Confidential

---

**Rule of Thumb** Any privileged or proprietary information must be maintained in confidence in order to maintain its confidential status. Company records must establish confidentiality of information in first instance AND show confidentiality has been maintained.

Even if personal information is shared, it is still personal information.

All confidential information can be shared on a need-to-know basis:

Within Company

Outside Company

# Privileged Information

---

- Information that is subject to a recognized, i.e., explicit privilege, in statute or case law
- Many types of privileges are recognized in the law, but not all are relevant for this issue
  - Priest/Penitent
- Creation of law of privilege represents a public policy decision
- Fair amount of consistency between various states' and federal rules

# Types of Privileged Information

---

- Attorney-Client Communication
- Attorney Work Product
- Trade Secrets
- Settlement discussions

# Attorney-Client Communications

---

- Attorney-Client Communication
  - Communications between client & counsel
  - Communications between client & counsel's agent
  - Communications between client's agent & counsel

# Attorney Work Product

---

- Attorney Work Product
  - Must be the work product of an attorney acting on the client's behalf
    - May include work in anticipation of litigation
    - May include work prepared while attorney is acting in non-litigation capacity
- Two kinds of attorney work product
  - Absolute: For a writing that reflects an attorney's impressions, conclusions, opinions or legal research or theories (aka opinion work product)
  - Qualified: For everything else

# Trade Secrets

---

- In a litigation context, rule is that the secret must be described “with sufficient particularity to separate it from matters of general knowledge in the trade...and to permit the defendant to ascertain at least the boundaries within which the secret lies.”
- Statutes may override traditional trade secret protections.

# Settlement Discussions

---

- Applies to Settlement & Mediation Discussions
- Protected from discovery or admission into evidence in any civil action to establish the purported liability of any defendant
- Purpose is to protect an interest in early and out of court settlements

# Types of Personal Information

---

- Insurance Information and Privacy Protection Act
  - Personal Information
  - Privileged Information
- Gramm-Leach-Bliley Act (GLBA) and state rules enacted in response to GLBA
- Health Information Portability and Accountability (HIPAA)
- Statutes related to particular medical related conditions and issues
  - AIDS/HIV
  - Genetic testing
  - Mental Health

# Insurance Information & Privacy Protection Act

---

- Based on a model law, and enacted by a minority of jurisdictions prior to advent of federal legislation.
- In California, the insurance privacy laws permit disclosure in the following situations:
  - To a person other than an insurance institution, agent, or insurance-support organization, provided such disclosure is reasonably necessary...(2) to enable such person to provide information to the disclosing insurance institution, agent or support organization for the purpose of...(B) Detecting or preventing criminal activity, fraud, material misrepresentation or material nondisclosure in connection with an insurance transaction....
  - To an insurance regulatory authority; or
  - To a law enforcement or other governmental authority pursuant to law.
  - As otherwise permitted or required by law....

# GLBA

---

- GLBA protects “Nonpublic personal information,” which means personally identifiable financial information:
  - (i) provided by a consumer to a financial institution;
  - (ii) resulting from any transaction with the consumer or any service performed for the consumer; or
  - (iii) otherwise obtained by the financial institution.
- Does not include publicly available information.
- Does include any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any nonpublic personal information other than publicly available information; but
- In terms of compliance, there are two key rules under the GLBA – the Financial Privacy Rule and the Safeguards Rule.

# GLBA – Financial Privacy Rule

---

- Requires financial institutions to provide a privacy notice to customers, at the time the consumer relationship is established and annually thereafter, which delineates the categories of nonpublic personal information the insurer collects and discloses and the categories of nonaffiliated third parties to whom the institution discloses this information.
- The privacy notice must:
  - explain the information collected about the consumer, where that information is shared, how that information is used, and how that information is protected.
  - identify the consumer's right to opt-out of the information being shared with unaffiliated parties per the Fair Credit Reporting Act.
- Should the privacy policy change at any point in time, the consumer must be notified again for acceptance.
- Each time the privacy notice is reestablished, the consumer has the right to opt-out again.
- The unaffiliated parties receiving the nonpublic information are held to the acceptance terms of the consumer under the original relationship agreement.

# GLBA – Safeguards Rule

---

- Requires financial institutions to develop a written information security plan that describes how the company is prepared for, and plans to continue to protect clients' nonpublic personal information. (The Safeguards Rule also applies to information of those no longer consumers of the financial institution.)
- This plan must include:
  - Denoting at least one employee to manage the safeguards;
  - Constructing a thorough [risk management] on each department handling the nonpublic information;
  - Develop, monitor, and test a program to secure the information;
  - Change the safeguards as needed with the changes in how information is collected, stored, and used.

# GLBA - Exceptions

---

GLBA contains several general exceptions for disclosure, including:

- to protect against or prevent actual or potential fraud, unauthorized transactions, claims, or other liability;
- to the extent specifically permitted or required under other provisions of law and in accordance with the Right to Financial Privacy Act of 1978 [12 U.S.C. 3401 et seq.], to law enforcement agencies (including a Federal functional regulator, the Secretary of the Treasury with respect to subchapter II of chapter 53 of title 31, and chapter 2 of title I of Public Law 91–508 (12 U.S.C. 1951–1959), a State insurance authority, or the Federal Trade Commission), self-regulatory organizations, or for an investigation on a matter related to public safety;
- to comply with Federal, State, or local laws, rules, and other applicable legal requirements; to comply with a properly authorized civil, criminal, or regulatory investigation or subpoena or summons by Federal, State, or local authorities; or to respond to judicial process or government regulatory authorities having jurisdiction over the financial institution for examination, compliance, or other purposes as authorized by law.

# Overview of Health Insurance Portability and Accountability Act of 1996 (HIPAA)

---

- Commonly referred to as the HIPAA Privacy Rule and the HIPAA Security Rule.
- In effect since 2003 (Privacy Rule) and 2005 (Security Rule).
- Privacy and Security Regulations were also promulgated by the Department of Health & Human Services.
- **Privacy Rule General Rule:**
  - A “Covered Entity” may not use or disclose Protected Health Information (“PHI”) without an individual’s authorization unless that use or disclosure otherwise is permitted under the Privacy Rule.
- **Security Rule General Rule:**
  - A “Covered Entity” must implement administrative, physical, and technical safeguards to protect the security of electronic PHI (“ePHI”).

# What HIPAA protects

---

- **Protected Health Information (“PHI”) / Individually Identifiable Health Information:**
  - Information (including demographic information).
  - Created or received by a health care provider, health plan, employer, or health care clearinghouse.
  - Relating to:
    - the past, present, or future physical or mental health or condition of an individual;
    - the provision of health care to an individual; or
    - the past, present, or future payment for the provision of health care to an individual.
  - Identifying the individual or there is a reasonable basis to believe that the information could be used to identify the person.

# Who must comply with HIPAA

---

- **“Covered Entities” :**

1. Health Care Providers (who submit claims electronically) – e.g., hospitals, physicians, dentists, nursing homes, pharmacies.
2. Health Plans – e.g., health insurance companies, HMOs, employer group health plans.
3. Health Care Clearinghouses -- Entities that translate data for another entity from nonstandard to standard and vice versa.

# Who must comply with HIPAA, cont'd.

---

- **“Business Associates” (BA):**

- A person or entity who performs activities or functions or provides services for, or on behalf of a Covered Entity that involves disclosure of Protected Health Information to the person or entity.
- BAs are not directly required to comply with the HIPAA Privacy Rule. Rather, a Covered Entity must enter into business associate agreements with each BA.
  - BAs must provide “reasonable assurances” that they will appropriately safeguard the health information.
  - BA Agreements have a number of required provisions as set forth in the Privacy and Security Rules, many of which mirror certain requirements of the Covered Entity.
- **Beginning in February 2010**, BAs must comply directly with the HIPAA Security Rule.
- If a BA needs to disclose PHI to another person or entity to assist the BA in providing services to the Covered Entity, the BA must ensure that that person or entity agrees to the same restrictions the BA agreed to in its BA agreement.

# HIPAA's Privacy Rule

---

- **General Rule:**
  - A “Covered Entity” may not use or disclose Protected Health Information (“PHI”) without an individual’s authorization unless that use or disclosure otherwise is permitted under the Privacy Rule.
- **Examples of Permitted Uses and Disclosures:**
  - To the individual or personal representative
  - To the Department of Health & Human Services for compliance
  - “Incident to” another permitted use or disclosure
  - For Treatment, Payment and Health Care Operations Purposes
  - Law Enforcement Purposes, Public Health Purposes, Judicial and Administrative Proceedings
  - Pursuant to an authorization
    - HIPAA Authorizations have specific provisions that must be included in the authorization.

# Disclosure of PHI under HIPAA

---

- PHI may also be used or disclosed for judicial or administrative proceedings if the use or disclosure is made in response to a court order, administrative tribunal order, subpoena, discovery request, or other lawful process.
  - Insurer may use or disclose PHI in the course of any judicial or administrative proceeding.
  - If there is another federal or state statute or administrative rule which requires a covered entity to disclose PHI to the state insurance regulator, HIPAA Privacy Rule permits the disclosure.
- It is important to note that the Privacy Rule permits a covered entity to "use or disclose protected health information to the extent that such use or disclosure is required by law and the use or disclosure complies with and is limited to the relevant requirements of such law."
  - In practice, the disclosure must be limited to what is required by the statute or regulation. Disclosure of more information than is required by law is not permitted.

# Types of Proprietary Information

---

- Loosest category, but generally revolves around trade secrets and intellectual property
- Includes any information where resources, expense and specialized knowledge have gone into development of information used for business purposes
- This sensitive information is owned by a company and gives the company certain competitive advantages
- Information may belong to
  - Insurer
  - Insurer's vendors

# A word about internal audits

---

- Defined
- Serves a useful purpose for companies
  - Self-monitoring
  - May be helpful to present information to regulators
- Regulators generally do not request
- But, internal audits are not privileged in the majority of jurisdictions, including California

# Regulator Authority to Request Information

---

- Authority is located in Statutes
- Scope of authority granted also represents public policy decision
  - Prevention of Fraud
  - Importance of Regulation

# Regulators' Authority to Obtain Information

---

- Power to Investigate
- Power to Subpoena
  - Regulated entities
  - Non-regulated entities
- Power to Examine
  - Market Conduct
  - Financial Exams
  - Holding Company Exams
- Discovery in Administrative Hearing Context

# Investigation & Subpoena Authority

---

The commissioner has the power to issue subpoenas and subpoenas duces tecum on any subject touching insurance business in aid of the commissioner's duties, whether in the context of an administrative proceeding or for purposes of an investigation or inquiry.

Witness Interviews

Public Hearings

# Market Conduct Exams

---

- Conducted by regulators in every jurisdiction
- Covers range of insurer activities
  - Advertising/Marketing
  - Rating & Underwriting
  - Claims Handling
  - Fraud/SIU

# Financial Exams

---

- Insurance Commissioner has broad authority to examine the books and records of insurance companies. On-site financial examination generally is conducted once every three years to five years while off-site examination in the form of financial analysis is done regularly on quarterly and annual basis.
- Documentation requested can be from:
  - a. Internal sources
  - b. External Sources

# Holding Company Act Examination

---

- Under the Holding Company Act, the commissioner can require production of records, books, and other information in the possession of the company's affiliates as part of an examination of the company's financial condition.
- This power may be exercised only if the general examination is inadequate or if the interests of the contract holders are being adversely affected.

# Discovery in Administrative Hearing

---

- Each state, including California, has an Administrative Procedure Act (APA) that grants limited discovery rights as part of the preparation for a hearing.
- The parties can seek discovery of documents and witness identifications from the other parties.
- A party can also subpoena documents from non-parties.
- Discovery requests on other parties must be served within 30 days of service of the initial pleading or within 15 days of a subsequent pleading.

# Other Sources of Information

---

- Other regulators
  - NAIC
  - Other State Agencies
- Insureds/Claimants
- Plaintiff's Bar
- Requests for Information to Industry or Specific Companies
- Press/Media Coverage

# Regulators' Authority to Enforce Requests

---

- Informal Actions by Department
  - Follow up requests
  - Expanding scope of request
  - Initiating more formal types of requests
- Formal Actions by Department
  - Extremely rare
- Referrals to other Law Enforcement Agencies

# Statutory Penalties – Cease and Desist Order

---

- The commissioner can issue a cease and desist order to a company in the case of a violation of law.
- The commissioner has the authority to issue an order as may be reasonably necessary to correct, eliminate, or remedy the conduct – therefore, the order can merely require the company to cease and desist from the improper conduct but also can be broader and could include an order to discontinue business in California until the company can demonstrate improvements.
- The commissioner can issue the cease and desist order before holding a hearing if necessary to avoid irreparable loss or injury but otherwise must hold a hearing before issuing the order. Even in the case of an emergency cease and desist order, the respondent has the right to request a hearing after the order is issued.
- A hearing on a cease and desist order is held before a Department of Insurance hearing officer, generally a Department staff attorney deputized for this purpose, and is not subject to the Administrative Procedures Act. The usual rules of evidence do not apply.
- Violation of a cease and desist order subjects the company to a fine not to exceed \$100 for each day of noncompliance up to \$5,000 and suspension of the company's license.

# Statutory Penalties – Conservation Order

---

- The commissioner can seek an order of conservation or liquidation of a company that is found to have violated California law.
- A conservation order results in the commissioner taking title to all of the company's assets and taking control of its operations.
- A conservation order is usually used in cases of financial hazard and is not common in the market conduct context, but it is a remedy available to the commissioner in extreme cases.

# Material Deficiency

---

- A company must continue to comply with the requirements for issuance of its certificate of authority, including competency, character and integrity of management, prompt and fair adjustment of claims, prompt and full payment of claims, and fairness and honesty of methods of doing business.
- A finding of material deficiency in any of these items can result in proceedings to suspend or revoke the company's certificate of authority.

# License Revocation/Suspension

---

- The commissioner may suspend the company's license for conducting its business fraudulently, for not carrying out its contracts in good faith, and for habitually compelling claimants to either accept less than the amount due under the contract or resort to litigation to secure payment of the amount due.
- A fine may also be imposed in lieu of suspension.

# Informal Penalties

---

- Once a company has a bad reputation with the Department, the Department has the ability to “blacklist” the company.
- Blacklisting can take many forms, including declining to issue approvals to the company, such as approvals to issue dividends or other holding company act approvals and license amendments.
- Blacklisting can include multiple market conduct examinations as well as subpoenas and other investigatory techniques that are not traditionally designed to be punitive in nature but permit the commissioner to delve into details of the company’s operations in a way that can be expensive and inconvenient for the company.
- Reputational damage with other regulators.

# Attorneys General/District Attorneys

---

- Most commissioners including, California, are authorized to refer certain matters to the state Attorney General or a District Attorney for enforcement.
- AGs may also initiate actions on their own
  - Investigations
  - Civil Investigative Demands
  - Subpoenas
  - Enforcement Actions
- AG/DA enforcement actions are venued in state courts, and would be subject to normal discovery rules.

# Legal Guidelines

---

- Laws recognize some instances where privileged information can be produced to regulator without negative repercussions for company
  - Generally applies to personally identifiable and protected information for claimants and insureds
- However, laws creating privilege also create conflicts with regulator's ability to review companies
  - Failure to provide guidance on how to resolve conflicts
  - Failure to protect confidentiality once information is produced
- An area that is ripe for further public policy discussion

# Regulators' Ability to Maintain in Confidence

---

- Set by statute
- May be subject to regulator discretion
- Importance of usual regulator protocols and procedures

# What happens if confidential information is provided to the regulator?

---

- *May* be able to produce trade secret information without waiving privilege.
- Regulators generally have authority to obtain personal information.
- However, case law is that production to regulator generally waives privilege.

# More about what happens if confidential information is provided to the regulator.

---

- Case law is that production to regulator waives privilege... unless there is duress or coercion.
- Standard for duress is high.

# Practical Considerations

---

What does it mean if the regulator has what used to be confidential information?

- Can be disclosed by the Commissioner
  - To other regulators
  - Press Releases
  - Pleadings
  - Other
- Can be requested from the Commissioner
  - Public Records Act Request
  - Subpoenas in Civil Litigation

# Insurer's ability to resist requests

---

- Wait and see
- Refuse to produce
- Attempt to narrow scope of request
- Force a subpoena, which could be subject to a motion to quash

# Best Practices – Establishing and Maintaining Confidentiality

---

- Develop Protocols and Procedures to identify and maintain confidential information
  - Who has access to information
  - Those with access understand confidential status
  - Consider need to document v. conducting verbal communications
- Consider involvement of counsel early on in the process
- Whenever possible, identify confidential information as such at the time of creation and when keeping records of the information
- Settlement agreements with insurance claimants should consider possibility of regulator requests

# Best Practices – Responding to Regulator Requests

---

- Make sure you understand scope of request – regulator may not intend or want to obtain confidential information
- Clearly identify to the regulator what information is confidential and why
- Consider asking regulator to issue a subpoena
- Consider compromises
  - Produce some or summary information
  - Ask for confidentiality agreement
  - Have regulator review information, but not take any of the documentation, etc., into custody
  - Ask regulator to help company establish coercion

# Practical Experience

---

- NAIC guidance counsels regulators to try to avoid requests for privileged documents
- Most companies reach a compromise with their regulators
- Companies also compromise with AG's, but are more likely to involve court in the process than in the case of a regulator request
- If a court is involved, there will be a public record of existence of information unless company is able to obtain a court order placing the matter under seal
- When forced to choose between regulators' rights of investigation, and privilege, courts, especially federal courts, are generally supportive of the attorney-client privileges
- For attorney work product, courts are more supportive if the information sought reflects opinion work product
- Regulators are very diligent about protecting personal information, although they may use that information to contact an individual to investigate a matter further
- Trade secret information is least often in issue

# Questions & Answers

---

**Elizabeth Tosaris, Esq.**

Sonnenschein, Nath & Rosenthal LLP

525 Market Street, 26<sup>th</sup> Floor

San Francisco, CA 94105

415 882 2449

[etosaris@sonnenschein.com](mailto:etosaris@sonnenschein.com)

[www.sonnenschein.com](http://www.sonnenschein.com)



Sonnenschein  
SONNENSCHN NATH & ROSENTHAL LLP