Safeguarding Non-Public Personal Information

A Guide for Independent Agents and Brokers

An Agents Council for Technology[1] Report

October 5, 2004

This report is not intended to provide specific advice about individual legal, business or other questions. It was prepared for use as a guide, and is not a recommendation that a particular course of action be followed. If specific legal or other expert advice is required or desired, the services of an appropriate, competent professional, such as an attorney or consultant, should be sought.

Overview

American citizens are becoming increasingly concerned with the privacy of their health and other personal information that is used, transferred, and retained by a multitude of different businesses. As a result, we have seen the enactment of federal and state laws, such as **Health Insurance Portability and Accountability Act ("HIPAA")[2], Gramm-Leach-Bliley[3], the Fair Credit Reporting Act[4],** and various laws which are all designed to regulate and protect this non-public personal information. In addition, federal and state government agencies that administer these laws have issued regulations concerning these privacy protections. ***COMPLIANCE with these laws is NOT AN OPTION for independent agencies and brokers. Failure to Comply can result in Significant Penalties and Liability which may not be covered by insurance.***

The purpose of this ACT report is to heighten agencies' awareness about the importance of taking steps within their businesses to safeguard the privacy of non-public personal information about their clients and prospective clients, whether it be the individually identifiable medical information that is governed by HIPAA or other non-public personal information that is impacted by other federal and state laws. ***This report is not a legal analysis or intended to provide a***

---

[1] The Agents Council for Technology (ACT) was formed by the Independent Insurance Agents & Brokers of America (IIABA), and its membership is composed of agents, user groups, carriers, vendors, and industry associations. ACT's mission is to encourage and facilitate the most effective uses of technology and workflows within the Independent Agency System. Additional information on ACT as well as its various reports and business tools are found at http://www.independentagent.com/act.

[2] A detailed discussion of HIPAA and its Privacy Rule are beyond the scope of this report. See the legal analysis published by IIABA entitled HIPAA Privacy Rule Effective April 14, 2003, Frequently Asked Questions and Answers found in the ACT HIPAA and Privacy Supplement for a detailed discussion of HIPAA and how it applies to independent agents.

[3] A detailed discussion of the specific requirements of Gramm-Leach-Bliley on independent agents is beyond the scope of this report. A legal analysis of this law and its implications for independent agents is available to IIABA members at www.independentagent.com in the Legal Advocacy section.

[4] A detailed discussion of the specific requirements of the Fair Credit Reporting Act is beyond the scope of this report. An IIABA legal analysis entitled Fair Credit Reporting Act Compliance Guidelines for the Use of Driving Records, Consumer Reports and Credit Scores, January 3, 2003, is available to IIABA members at www.independentagent.com in the Legal Advocacy section.

detailed discussion of individual privacy laws. (See footnotes below for references to such resources.) Rather, it is intended to assist agents and brokers in formulating an overall privacy strategy for their businesses along with appropriate policies and procedures.

In Prosecuting Violations of these laws, **the Government**, in ascertaining that the requirements of the specific laws have been adhered to, **may want to see that the agency has**, to the extent required by applicable laws:

- ✓ ***Acted*** to protect the privacy of this personal information by adopting appropriate policies and procedures
- ✓ **Restricted** access to only those employees who need to see the information
- ✓ **Trained** the agency's employees in these policies and procedures
- ✓ **Audited** compliance and corrected instances of non-compliance
- ✓ **Documented** all of these steps.

These laws and their regulations are still relatively new, and thus, their precise applications to various agency practices are subject to interpretation and will continue to evolve.

Traditionally, most independent agents and brokers have been careful with their clients' personal information. It is good business. The risks have become a lot greater in recent years, however, because now this information is stored electronically within the agencies and therefore may be more accessible to more agency employees. In addition, the agency management systems themselves are more exposed to the external world through the Internet. Couple these risks with the unfortunate fact that there are more individuals out there today actively seeking to steal identities of unsuspecting people and to capitalize on them.

The policies and procedures introduced in this report are offered to help agencies develop their strategies to manage these risks. They also can help position the agency to meet the emerging expectations of their clients for privacy. In this light, **Agency Principals** should establish privacy protection as a **Priority** for the agency, take the steps necessary to implement the protections, and then promote it as a specific benefit provided by the agency. ***In other words, approach the issue positively and pro-actively because it is good business.*** Such an approach has the added advantage of minimizing the agency's exposure to prosecution, or liability, and negative public relations for failure to safeguard private personal information.

The next section outlines some key principles agents and brokers should consider in their privacy protection policies. Keep these principles and common sense in mind—along with the specific statutory and regulatory requirements-- as you design and implement your agency's privacy policies and procedures. Designing privacy procedures involves a balancing process that also must allow the agency to continue to function effectively as a business that derives benefit from its systems and electronic interactions with its trading partners.

Following the "Key Principles" section, the report discusses a number of privacy tips for the automated insurance office. The report then addresses how HIPAA typically impacts independent agents and brokers and then includes helpful employee training and compliance material, introductory material regarding employee benefits workflows that are likely to be affected by the law, and some high level security issues to address.

IIABA and ACT offer two additional resources: 1) the ACT HIPAA & Privacy Supplement, which contains sample employee benefits workflows and identifies those workflows which are likely to be impacted by Protected Health Information, more detailed security information and the HIPAA FAQs (developed by IIABA's Office of General Counsel); 2) the Memorandum on Final HIPAA Privacy Regulations (also developed by IIABA's Office of the General Counsel)[5].

Key Principles

Agency and broker principals may want to develop an overall privacy policy that is designed to comply with the various privacy laws, rather than trying to adopt multiple policies based upon the requirements of each law. Unique components include things such as securing customer authorization before ordering credit reports (Fair Credit Reporting Act), providing annual notices to customers regarding the agency's privacy policy and rights to opt out of most disclosures to third parties (Gramm-Leach-Bliley Act), etc.

These policies and procedures should apply to **Employee Non-Public Personal Information** as well as to **Prospect /Customer Information**.

Agents and brokers may want to appoint a privacy officer who has a good knowledge of overall agency operations and charge that individual with developing a detailed understanding of the various privacy laws. That individual can manage the staff team developing and then implementing the privacy policy and procedures, oversee the audit process for compliance, and receive privacy-related complaints and problems.

Agents and brokers also may want to appoint a security officer to oversee the agency's security policies and procedures in order to protect the agency's information from both external and internal threats-- whether the information is in electronic or paper form, or conveyed orally.

Limiting access to non-public personal information and individually identifiable medical information to only those employees who have a need to see it is another privacy protection agents and brokers may want to implement. This principle is commonly seen in the various privacy laws. How can the agency's systems be "locked down" to limit this access to the appropriate employees? What procedures can be adopted by the mailroom to avoid viewing of this sensitive information? What steps can be taken with the technology staff who have broad access to systems information or with **Vendors** who have access to the agency's systems and information? What procedures should be adopted to assure that individual employee passwords are safeguarded and that the agency immediately terminates a departing employee's access both to the agency's systems as well as the systems of the agency's trading partners? What communications policies are put in place so the mail and faxes are used to send private health and personal information, rather than e-mail which is not a confidential medium unless sent in **Encrypted** form?

[5] This report is available to IIABA members at www.independentagent.com in the Legal Advocacy section.

Agents and brokers may want to raise awareness with every agency employee regarding the importance of safeguarding all non-public personal information and individually identifiable health information and employee passwords, and provide training to both existing and new staff as they come onboard with regard to the agency's privacy policies and procedures. A sample employee training memo, geared specifically to HIPAA, is attached at Appendix A. Agency employees can be asked to commit in writing to safeguard the confidentiality of all protected information, to access it only when they have a legitimate business purpose to do so, and to use the information only for the business purpose for which it was intended to be used.

Employees with access to non-public personal information and/or individually identifiable health information should take steps to keep it out of view of fellow employees whether it is on the computer or on paper, especially when they are away from their desk. In addition, they may want to create a procedure to verify a caller's identity before discussing private information with them. Employee reminders can be placed throughout the agency regarding the importance of the agency's privacy policies. Employees can also be asked to advise the privacy officer should they come across private information to which they should not have access, so that improved procedures can be considered.

It is important for agencies to consider the effectiveness of their privacy strategy. An audit of the implementation of their privacy policies and procedures is one way to measure a privacy policy's success. If an audit is conducted, written records of it, along with any problems found, and corrections implemented should be kept. This is exactly the type of information government agencies or others may be looking for if a privacy complaint were to be lodged that involves the agent or broker.

Privacy Issues in the Automated Insurance Office

Agents collect an extraordinary amount of information to secure coverage for a customer. Of special concern is sensitive information such as social security numbers and credit card information, as well as other non-public personal information and individually identifiable health information—all data that must be kept private. In the course of business, agents also must accumulate information that an individual might consider "private" regardless of its legal status as protected or unprotected – traffic tickets/accidents, lawsuits, driver's license revocations, financial and credit information, payroll data, etc.

One security measure commonly used is password protection for access to computers, networks, individual database records, or other files. Agency management systems and servers can offer multiple levels of security access for computerized data records, and these features can be implemented. Safeguards can avoid unauthorized access to "integrated" data systems.

Regarding general office workflows, any customer information on paper, which is subsequently scanned into the system and which is not required to be maintained in hard copy by a law or regulation, record retention policy or contract, can be shredded so that no information regarding the customer can be retrieved from the trash. File cabinets, if any, should not be accessible to unauthorized persons for any reason. File cabinets should be locked at the end of each workday, and files containing individually identifiable health information should be locked whenever an

authorized employee is not present at the file location. The fax machine can be checked regularly for any transmissions to ensure that no private customer information is left in the fax machine for other employees or customers to view. Any files or papers with non-public personal information or personally identifiable health information used for data entry should be secured as soon as possible.

Employees should have training on appropriate data collection processes. Data should be collected and used lawfully and fairly. Data should be held securely, including CDs and back-up tapes. Employees should only have access to appropriate data and should consider all customer data to be confidential.

If employees use laptops to create, store or process sensitive or confidential data, access control software can be installed to prevent unauthorized access. All sensitive or confidential data can be erased from diskettes before discarding them, giving them to someone else, or using them again for storing new information.

Employees that have computers connected to a Local Area Network or a mainframe computer should always remember to logout or lock access before leaving the workstation.

How does HIPAA Touch Independent Agents?

HIPAA safeguards private health information which is individually identifiable by imposing specific requirements on "Covered Entities." "Covered Entities" include:

- Health plans
- Healthcare clearinghouses
- Healthcare providers

Independent Agents are touched by the "Covered Entities" known as health plans.

When insurance agents **Sell** or service employee benefits insurance, they may be required to take steps to **Comply with HIPAA** requirements. If an insurance company or an employee benefits client has had the agency sign a **Business Associate Agreement**, the agency has become a **Business Associate** of the company or the client. As a Business Associate, the agency has accepted the responsibility to follow through on certain compliance requirements. The Business Associate Agreements agents have been signing typically incorporate HIPAA privacy and security provisions (45 CFR 160 through 164).

If the agency has signed a Business Associate Agreement, it has most likely promised, indemnified, warranted, made a covenant or ***Personally Indemnified*** that the agency is in ***compliance*** with specific HIPAA requirements. ***It is CRITICAL for Agency Principals to FULLY Understand the commitments they have taken on in signing various Business Associate Agreements along with whether their privacy policies and procedures fully cover these commitments.***

An insurance agency is also an Employer. Agencies as employers usually sponsor health plans for their employees. The health plans are Covered Entities and the agency/employer is the plan sponsor. As the Plan Sponsor, the Agency has the Responsibility to make sure the Health Plans are In **Compliance** with the HIPAA regulations. Health plans that must be in compliance include:

- **Group medical plan (HMO or PPO)**
- **Dental**
- **Vision**
- **Pharmacy/prescription**
- **Long Term Care**
- **Flexible medical spending account**
- **125 Plan**
- **HRA**
- **Employee Assistance Program**

An independent agency as an employer and plan sponsor must assess the group health plans sponsored and determine what is required to bring the health plan(s) into **Compliance**.

Employee Training and Awareness

Please see Appendix A for a sample agency HIPAA Employee Compliance Training Memo which provides a succinct explanation of HIPAA and how a particular agency is complying with it. It is important for agencies to customize this sample to take into account the specific aspects of their operations and how they handle Protected Health Information.

Impact of HIPAA on Benefits Departments Procedures

The ACT HIPAA and Privacy Supplement contains a useful tool for agencies to use to assess the aspects of their benefits workflows that might be impacted by HIPAA. This tool includes a sample benefits department's workflows and emphasizes those workflows that involve exposure to Protected Health Information (PHI). The day to day activities of a benefits department provides the opportunity for many exposures to PHI, and therefore several opportunities exist for improper viewing or release of this information. As discussed throughout this report, deliberate steps must be taken to protect this information. Once again, it is important for agencies to customize these sample workflows to reflect their specific operations and how they specifically handle Protected Health Information.

Safeguarding the Security of the Agency's Systems

Maximizing the security of the agency's information systems—whether it is electronic or paper information—is a critical part of protecting private client information. Here are some commonly found vulnerabilities that need to be evaluated for meeting the intent of HIPAA requirements:

1. Evaluate data access.
    a. Do you have a policy set for data to be accessed on a "need to know" basis?

b. Have you secured all databases and data storage to technically enforce said policy?

2. Evaluate ease of access to your building.
    a. Can guests at your agency walk around your building without escort and/or name badges?
    b. Do you log guests that visit your agency?

3. Evaluate access to your computer network.
    a. Consider shutting off open Ethernet ports in the office.
    b. Keep Wireless Access Points off of the trusted network (on your DMZ).
    c. Have a firewall that, by default, has all ports closed unless needed (and opened only to the IP addresses it needs to access).
    d. Consider any network access 'holes' (PPP, VPN, etc) on your network.

4. Evaluate policy on non-trusted devices and software.
    a. Can staff / guests attach personal laptops and hardware on your computers and network?
    b. Can staff / guests install software on systems, or open documents from CD / floppy?

5. Evaluate backup security.
    a. Are data backups completed daily?
    b. Are backups stored in a secure location?
    c. Are backups regularly stored off-site in an environmentally secure location?

6. Evaluate access to paper information.
    a. Are documents left on desks at the end of the workday?
    b. What security is placed on client charts / folders?

7. Evaluate policy on sharing of information.
    a. Is policy set on identity verification of callers?
    b. Is policy set on what types of information can be disseminated, and by what authority process?

8. Evaluate agency's password management policy.
    a. Do employees understand the importance of keeping their passwords private and not posting them on their monitors?
    b. Are procedures in place so that passwords of former employees are terminated immediately to all of the agency's systems and to the systems of the agency's trading partners?
    c. Does the agency follow the ACT guidelines[6] for password management?

---

[6] ACT's Password Guidelines are found at www.independentagent.com/act by clicking on the ACT Reports icon.

This report was prepared by the ACT HIPAA Work Group:

Chris Ball, Insource, Inc., Workgroup Chairman
Kay Barrett, IMA Financial Group
Ed Higgins, Thousand Islands Agency
John Higginson, Applied Systems
Johnmichael Monteith, Parker Smith Feek
Judi Newman, Phaze II Consulting
Fred Petters, Maritime Insurance Group
Wayne Sather, Maritime Insurance Group
Bonnie Schaller, Ten Eyck Group
Bob Slocum, The Slocum Agency
Gerri Tillbrook, The Hartford Insurance Group
Angelyn Treutel, Treutel Insurance Agency
Alison Zernik, Brown & Brown
Jeff Yates ACT Executive Director
Debra Perkins, IIABA Executive Vice President & General Counsel

Appendix A

HIPAA EMPLOYEE COMPLIANCE TRAINING MEMO

First of all, what is Protected Health Information ("PHI")? It is any information, including demographic data that relates to:

- the individual's past, present or future physical or mental health or condition,
- the provision of health care to the individual, or
- the past, present, or future payment for the provision of health care to the individual,

and the information identifies the individual or provides a reasonable basis that can be used to identify the individual. Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, social security number, zip code, etc.).

The purpose of HIPAA, in a nutshell, is to protect all such information for the benefit of individuals – respecting their right to privacy. [Agency Name] has always taken pride in protecting such information, but the government is now mandating that particular procedures be in place and that covered entities be in compliance with the new regulation. Therefore, [Agency Name] employees must be made aware of the new regulations; how the regulations impact [Agency Name] as a whole and individual employees/departments; written policies and procedures must be in place; training must be provided to employees; and compliance must be maintained.

The Employees Benefit Department, IT Department and employees handling mail are largely affected by HIPAA. Thus, they will have more in-depth training than most other employees. If any employee comes across PHI accidentally or incident to a transaction, he or she must follow appropriate procedures when handling such information which will be discussed below.

Employees agree as follows:

Not to Use or Disclose PHI Unless Permitted: Employee agrees to not use or further disclose Protected Health Information other than as permitted or required by an Agreement or as required or allowed by law.

Use Safeguards: Employee agrees to use reasonable safeguards to prevent use or disclosure of the Protected Health Information other than as allowed by an Agreement or as otherwise allowed by law.

Mitigation of Harmful Effects: Employee agrees to mitigate, to the extent practicable, any harmful effect that is known to employee from a use or disclosure of Protected Health Information by an employee in violation of the requirements of an Agreement.

Report Inappropriate Disclosures of PHI: Employee agrees to report to his or her manager, who in turn will report the same to the Covered Entity, any use or disclosure of the Protected Health Information not permitted by an Agreement or by law.

The following safeguards and procedures have been implemented to assure compliance with HIPAA:

- All mail directed to the Employee Benefits Department or an individual within the Department, will simply be date stamped and delivered to the Department without the same being opened. If any mail is directed to [Agency Name] in general, but contains PHI that is discovered when opened, it shall be placed in an envelope labeled "Employee Benefits" and delivered accordingly.

- All incoming faxes that are received on a fax machine other than the dedicated fax machine for the Employee Benefits Department, shall be placed in an envelope labeled "Employee Benefits", and an e-mail should be sent the appropriate person(s) indicating the receipt of the fax and the placement in his or her mailbox.

- Any documents needing to be scanned should be placed in a similar envelope as indicated above and directions given to the appropriate front-desk person. Once the document has been scanned and sent via e-mail to the appropriate person, it should be deleted from all locations at the front computer.

- A fax/copy machine/printer has been purchased which is dedicated to the Employee Benefits Department. The business cards for Employee Benefits employees have been revised to reflect the new fax number. This new fax number will also be added to all directories (i.e. Intranet, Human Resources, etc.).

- Any print jobs by the Employee Benefits Department will either be sent to this new fax machine or sent to another printer (i.e. if color is necessary or it is a rather large job), with the sender to immediately go to the specified printer to wait and retrieve the print job.

- Locked file cabinets, overheads, etc. located in the Employee Benefits Department will be utilized each night for safekeeping. During the day, EB personnel will be very cautious to not leave work open on their desk and to place working documentation in cabinets as is reasonably feasible when leaving their work area.

- All files currently stored in the basement storage room, will be prepared and shipped for off-site storage. A Business Associate Agreement should be executed by a representative of the off-site storage facility. All other files, books, information, etc. will be stored in the EB Dept. in locked cabinets. If the need arises for additional storage space in the future, applicable storage space will be sought.

- Compliance issues relating to the computer (i.e., file organization, passwords, etc.) have been coordinated by IT staff. Basically, the EB Dept. at each location should have passwords different from the common ones everyone else utilizes. All information should be stored in a secured location, accessible only to the EB Dept.

- Training is being performed by [Agency Employee] to all EB personnel, mail people and IT people initially via either in person or video conference. All other employees will be trained at a different time, but as soon after the initial training as possible.