UnumProvident

# Privacy *Guidebook*

A guide for plan administrators

# Table *of Contents*


## Part I: The issue of privacy

## Part II: Privacy in the workplace

a. Drug testing/screening
b. References
c. Background checks
d. Workplace monitoring
e. Identity theft

## Part III: Insurance Information and Privacy Protection Act

a. Background
b. Application

## Part IV: Gramm-Leach-Bliley Act

a. Background
b. Pretexting

## Part V: The HIPAA Privacy Rule

a. Covered information
b. Covered entities
c. Covered plans and benefits
d. Self-insured employee benefit plans
e. Individual rights
f. Federal civil and criminal penalties
g. UnumProvident's compliance with HIPAA
h. Electronic data interchange

## Appendix

Covered entity document

# Part I: The issue of privacy

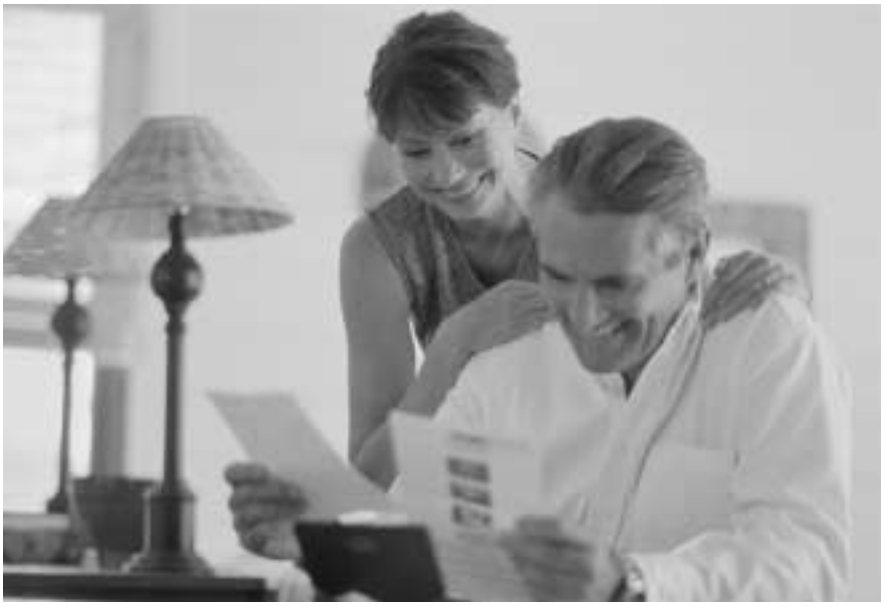
**Today's heightened** use of technology, in both our personal and professional lives, has made privacy – specifically, the protection of electronically stored and transferred personal information – a key societal issue. Emerging concerns about online privacy, identity theft, the protection of health-related personal information, etc., has led to a mix of new laws and regulations that affect healthcare providers, insurance companies and, of course, employers.

## Every coin has two sides

As consumers, we want our personal information to be kept confidential, but we also want the advantages of online services and the ease and quick turnaround times that electronic data transfer makes possible. As employers, however, priorities shift to an appreciation for electronic assistance in monitoring employee actions, quality control and theft prevention. The challenge for employers – to prevent claims of privacy invasion – is to balance business needs with each employee's reasonable expectation of privacy.

## How this guidebook can help

The purpose of this guidebook is to highlight privacy issues and regulations that might affect your workplace, providing you with a basic reference tool and, whenever possible, directing you to government agencies who can provide you with further information on specific regulations. This guidebook is not intended to give advice or to replace your legal counsel. If you have specific legal questions, you should consult your attorney.



## Privacy issues in the news

**Cyber scams –** An article from the Federal Trade Commission, Consumer Credit File Privacy: The Real Deal, warns consumers of an e-mail that encourages recipients to call an 800 number and give their social security number to prevent the four major credit bureaus from releasing their credit information.[1]

**Video surveillance –** Primarily used for theft prevention, video monitoring has caused controversy when used in areas where customers and/or employees have an expectation of privacy – such as restrooms or locker rooms.

**Identity theft –** Information found in old personnel records at Ligand Pharmaceuticals in San Diego was used by an employee to rent property, open cellular telephone accounts and even to set up credit card accounts.[2]

**Facial Recognition Biometrics –** This technology allows law enforcement officials to recognize individuals through video monitoring, using the unique measurements of facial geometry – in the news following its use at the 2001 Superbowl in Tampa, Fla.

## Privacy issues affecting the workplace

Privacy issues in the workplace are a deepening trend as employers are working to balance business needs with employee expectations. Some of the more obvious areas of concern include the safekeeping of personnel records and keeping current on the various privacy laws such as the Gramm-Leach-Bliley Act and the HIPAA Privacy Rule. But some privacy topics can be more controversial, including drug testing/screening, providing employee references and conducting background checks for prospective employees.

Regardless of the issue, employers have an obligation to respect employees' privacy while also considering their safety – and they must always operate in the best interest of the company. Sometimes it is difficult to achieve this balance.

**Consider the following issues:**

**Drug testing/screening –** Employers seek to protect themselves against hiring or retaining employees with drug habits that could pose a danger in the workplace. Employees, however, sometimes see drug testing as an invasion of their privacy and can also be concerned about the possibility of false positive test results. Employers who conduct drug tests or screens must enforce their policy in a way that doesn't create a risk for legal claims.

**References –** Typically employers don't hesitate to provide a reference for a former employee who leaves in good standing. But what about the marginal employee who has resigned or who has been fired? If you include potentially damaging information in any reference materials, you could position yourself for a defamation lawsuit. If you leave out information that could put another employer at risk – for example, concerning an employee who was fired for violent behavior – you are also at risk for legal action.

There are several options for providing references that you might consider. Many companies provide nothing beyond name, title and verification of dates of employment. Or, you can give only facts and not include information that is subjective or based on opinion – such as regarding an employee's perceived job performance. The one exception that many employers struggle with is the situation where an employee has been fired for violent behavior. It's important to decide how to respond to this situation before it happens. Having a specific company policy regarding employee references is recommended.

**Background checks –** For specific positions, a company may clearly need to conduct a criminal, ethical or financial background check. If you plan to use a third party to conduct these checks, you are required by law to get the prospective employee's consent in advance. The Fair Credit Reporting Act requires that if you are going to use the information provided by a third party as a basis for an adverse decision, you must provide the applicant with a notice of his or her rights under the law. The applicant is then given five days to refute the information before the decision is final. There is a risk that data files may contain erroneous information. This can be harmful to job applicants if the employer doesn't notify them of the results.

It is generally accepted that businesses need to monitor the workplace to assure quality control, assess productivity, control loss through theft, detect and prevent the sharing or selling of trade secrets, and guarantee a safe work environment for employees by detecting sexual harassment and violence among workers. Many companies bridge the gap between employee privacy and the company's need for monitoring by informing employees that monitoring is being conducted and also by not using video monitors in areas where employees tend to expect privacy.

**Workplace monitoring –** In most states, employers are not required by law to disclose to their employees that monitoring is taking place. And, in the few cases in which workers have filed lawsuits for privacy violations, the courts have largely decided in the employer's favor.

# Part II: Privacy in the workplace

**Identity theft** – Identity theft is another area where privacy issues can enter the workplace – especially if that theft is related to the maintenance of personnel records. One likely reason for the escalated occurrence of identity theft is the widespread use of the Social Security Number (SSN) as a means to uniquely identify a person. Every effort should be made to use and disclose all information about a person with great care, and this includes the use and disclosure of SSNs. If that type of information gets in the wrong hands, it can be devastating for employees as well as the company. According to the Federal Trade Commission, the average victim of identity theft spends 175 hours and $1,100 in out-of-pocket expenses for notarizing, postage, telephone calls, travel and even lost time from work, to correct the situation.[3]

With the adoption of the federal Identity Theft and Assumption Deterrence Act of 1998, identity theft became a felony. And according to TransUnion Credit Bureau, the number one underlying source of identity fraud is theft of employer records.[4] What can employers do to be prepared?

The most important safeguard is to have policies and procedures in place to protect the information you keep – both hard copies and electronic files. You should be able to show that you took reasonable care to safeguard your employees' personal information.

Here are some suggestions:

- Create awareness of privacy issues among personnel who have access to this information
- Keep files locked in a secure place
- Limit the number of people who have access to personnel files (especially temporary workers)
- Use password protected electronic files and change passwords often
- Shred trash that contains sensitive data
- Disguise mail that contains personal information

In addition to these suggestions, develop a plan of action in the event identity theft does occur in your business. If it happens, quickly notify affected employees. Set up toll-free phone lines for them to use when reporting the theft to the companies with which they have accounts. Each of the three major credit bureaus have dedicated fraud lines:

**Equifax – 1-800-525-6285**
**Experian – 1-888-397-3742**
**TransUnion LLC – 1-800-916-8800**

Individual states are beginning to respond to the issue of identity theft with applicable legislation. California, for example, has enacted a bill (SB 1386) that requires any organization (including employers) that owns or licenses computerized data that includes personal information to disclose any breach of the security of the system following discovery of the breach to any resident of California whose "unencrypted" information is believed to have been seen by an unauthorized person.[5] Companies who are not located in California, but who have employees in the state, may be required to comply.

The U.S. government's central website for information about identity theft is maintained by the Federal Trade Commission (www/consumer.gove/idtheft/). It is a good source of information for businesses and consumers with government reports, law enforcement updates and links to other helpful sites.

While Social Security Numbers (SSNs) are still part of UnumProvident's business process, we are aware of the security that we must provide in order to not misuse or disclose the SSN unnecessarily. As new laws are passed limiting the use or disclosure of SSNs, you can be assured that we will make changes where necessary to comply with the law. We encourage you to take the same position in order to protect your employees and your customers.

## Insurance Information and Privacy Protection Act (1982 Model Act)

*Background*

In 1982 the National Association of Insurance Commissioners (NAIC)[6] adopted the Insurance Information and Privacy Protection Model Act (1982 Act), which established guidelines for the disclosure of insurance consumers' personal information, including financial and health information. By October 2003, approximately 17 states had adopted laws based on the 1982 Model Act, and most states now have laws that address privacy issues of insurance consumers.

Although the 1982 Act does not regulate actions of plan administrators of group policies as such, it is helpful for plan administrators to understand the law's basic instructions concerning the uses and disclosures of information that covered employees disclose to an insurance company.

The 1982 Act established standards for the collection, use and disclosure of information gathered in connection with insurance transactions. Recognizing the need for insurance companies to have access to this information, as well as the consumer's right to privacy, the 1982 Act gives consumers the right to know what information is being gathered about them, to verify its accuracy and to limit the distribution of this information to others. There is also a provision guaranteeing a consumer's right to know the reasons for adverse underwriting decisions.

*Types of information it applies to:*

- Personal information – Includes any individually identifiable information gathered in connection with an insurance transaction; includes individual's name, address and medical records. It does not include privileged information (see below).
- Medical record information – Includes personal information that is related to an individual's physical or mental condition, medical history or medical treatment and is obtained from a medical professional or the individual's spouse or parent.
- Privileged Information – Includes any individually identifiable information that relates to a claim for insurance benefits, or a civil or criminal proceeding involving an individual and is collected in connection with, or in reasonable anticipation of, a claim or civil or criminal proceeding.

The 1982 Act also requires that insurance companies provide privacy notices to their insured customers. These privacy notices typically explain why the insurance company needs personal information, what they do with the information and the steps they take to protect the privacy of their customers.

The 1982 Privacy Protection Model Act applies to the following insurance products primarily purchased for personal, family or household purposes (non-commercial):

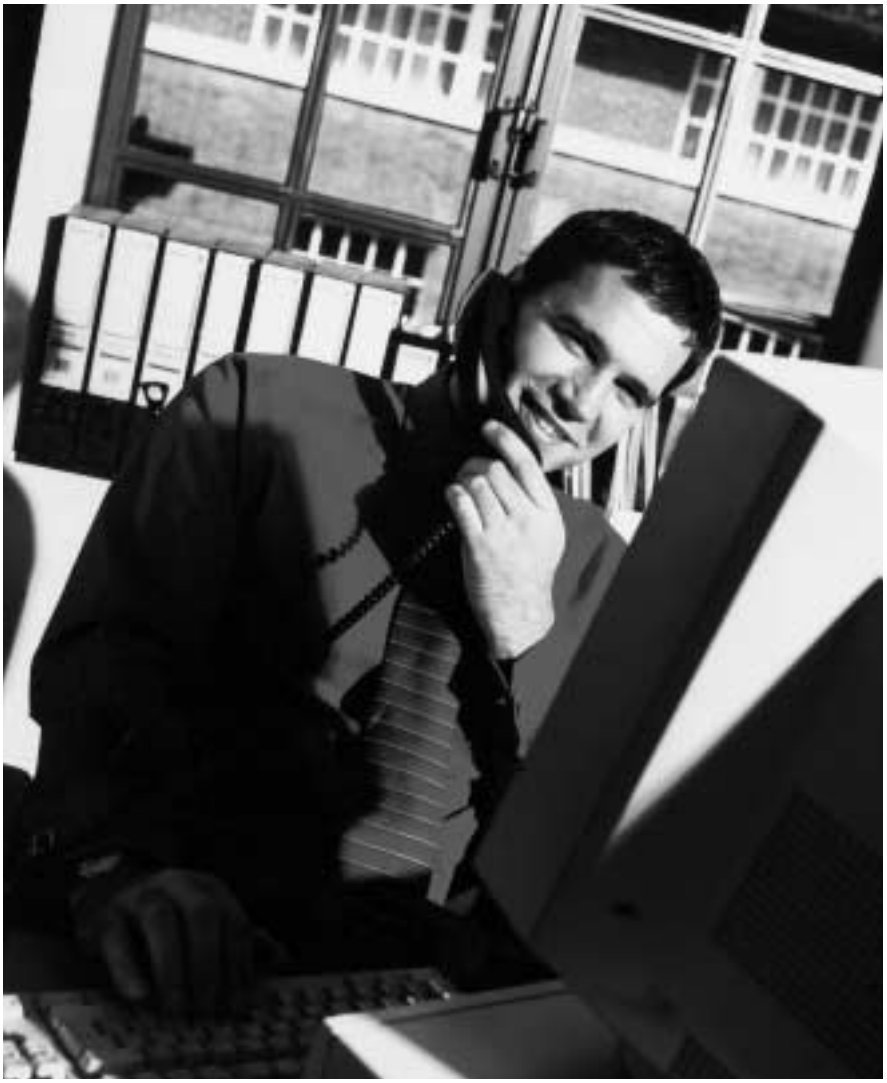
- Life
- Health (including long term care insurance)
- Disability
- Property
- Casualty

## Gramm-Leach-Bliley Act

### *Background*

The Gramm-Leach-Bliley (GLB) Act, a federal law enacted on Nov. 12, 1999, primarily addresses reforms to the financial services industry including concerns relating to consumer financial privacy. Enforcement of the privacy provisions of the GLB Act is by the Federal Trade Commission (FTC) and other government agencies (including state agencies) that regulate the financial industry. All covered businesses had to be in full compliance by July 1, 2001.

The GLB Act restricts certain disclosures of a financial institution customer's "nonpublic personal information" to nonaffiliated third parties. Covered financial institutions, including insurance companies, must annually send a notice about their information-sharing practices to customers. If a covered financial institution discloses nonpublic personal information to non-affiliates for certain purposes (for instance, marketing a non-financial product or service), that financial institution must inform customers that they may "opt out" if they do not want their information shared in that manner.



The GLB Act applies to businesses that are significantly engaged in financial activities. According to provisions established by the Federal Reserve Board, financial activities include:[7]

- Lending, exchanging, transferring, investing for others, or safeguarding money or securities. These activities cover services offered by lenders, check cashers, wire transfer services and sellers of money orders.
- Providing financial, investment or economic advisory services. These activities cover services offered by credit counselors, financial planners, tax preparers, accountants and investment advisors.
- Broker loans
- Servicing loans
- Debt collecting
- Providing real estate settlement services
- Career counseling (of individuals seeking employment in the financial services industry)

### *Pretexting*

The GLB Act prohibits "pretexting," or obtaining private information through false pretenses. This includes giving false statements and using impersonation to obtain consumers' private financial information. The law also prohibits the solicitation of others to engage in pretexting.

The FTC developed "Operation Detect Pretext" in 2001 following the enactment of the GLB Act. The agency screens websites and reviews print advertisements and notifies firms that might be in violation. As a result of this effort, the FTC has brought cases against individuals and companies that engage in the practice of selling consumer financial information.[8]

Certain actions are exempt from this particular subchapter of the GLB Act. The law does not apply to:

- any actions of a law enforcement agency in connection with the performance of its official duties
- an insurance company for investigation of insurance fraud
- financial institutions, when testing the security procedures for maintaining the confidentiality of its customers
- financial institutions that are investigating allegations of misconduct or negligence on the part of any officer, employee or agent of the financial institution
- recovering customer information that was obtained or received by another person using false pretenses
- the collection of child support judgments

If you are or may be a covered financial institution, check with your legal representative about GLB Act requirements before using or disclosing personal financial information about an individual. For additional information about the GLB Act, you can visit the FTC's website at www.ftc.gov. The website provides much information on the law, including written guidance on compliance issues that may be relevant to your business.

## UnumProvident's Commitment to Privacy

UnumProvident has adopted one privacy notice to comply with both the 1982 Act and GLB Act requirements. This notice is sent to all of our customers and can also be found on our website at www.unumprovident.com/aboutus/. Just click on Legal & Privacy Notices on the left of your screen, then click on Privacy Notice.

## The HIPAA Privacy Rule

*Background*

The HIPAA Privacy Rule was established to ensure that individuals' health information is protected while allowing the flow of information that is necessary for those individuals to receive proper care and treatment, as required by the Health Insurance Portability and Accountability Act of 1996. The rule sets standards concerning the use and disclosure of health information by covered entities, as well as establishing an individual's rights with regard to certain health information.

The majority of covered entities (health plans, health care providers and health care clearinghouses) were required to be in compliance with the HIPAA Privacy Rule by April 14, 2003.

To see the rule in its entirety, or for more detailed information on how it applies, visit the website of the Department of Health and Human Services (DHHS) at www.hhs.gov/ocr/hipaa.

## What information is covered by the HIPAA Privacy Rule?[9]

**Protected Health Information–** The HIPAA Privacy Rule protects all "individually identifiable health information" held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper or oral. The Privacy Rule calls this information "protected health information (PHI)."

Individually identifiable health information is 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
- the past, present, or future payment for the provision of health care to the individual
- identity of the individual or information for which there is a reasonable basis to believe it can be used to identify the individual

The Privacy Rule excludes from protected health information employment records that a covered entity maintains in its capacity as an employer and education and certain other records subject to, or defined in, the Family Educational Rights and Privacy Act, 20 U.S.C. §1232g.

**De-Identifiable Health Information–** There are no restrictions on the use or disclosure of de-identified health information. De-identified health information neither identifies nor provides a reasonable basis to identify an individual. There are two ways to de-identify information. These are (1) a formal determination by a qualified statistician; or (2) the removal of specified identifiers of the individual and of the individual's relatives, household members and employers. These are adequate only if the covered entity has no actual knowledge that the remaining information could be used to identify the individual.

**Health Care Clearinghouse (HCC) -** a public or private entity that either:

a. Receives health information from another entity in nonstandard format or containing nonstandard data and processes or facilitates the processing of it into standard data elements or a standard transaction; or

b. Receives a standard transaction from another entity and processes it or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving party.

Common examples of entities that may be HCCs include:

- Billing services
- Repricing companies
- Third party administrators

**Health Care Provider (HCP)-** a covered entity only if that HCP transmits health information in electronic form in connection with a HIPAA regulated EDI transaction.

For HIPAA EDI and Privacy purposes, a health care provider means:

a. The following entities:

- Hospital
- Critical access hospital
- Skilled nursing facility
- Comprehensive outpatient rehabilitation facility
- Home health agency
- Hospice program
- Certain funds paying for services provided by teaching hospitals or medical schools

b. An entity or person that provides medical or health services as defined in 42 U.S.C. 1395x(s) (located in the Appendix)

c. any other person or organization who furnishes, bills or is paid for health care in the normal course of business

**Health Care -** services or supplies related to the health of an individual. Health care includes, but is not limited to, the following: (1) preventative, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care and counseling, service, assessment or procedure with respect to the physical or mental condition, or functional status of an individual, or that affects the structure or function of the body; and (2) sale or dispensing of a drug, device, equipment or other item in accordance with a prescription.

### *The HIPAA Privacy Rule and self-insured employee benefit plans*

Any organization that provides health benefits to its employees or that is considering a change to a self-insured plan will need to review the provision of benefits, the structure of the plan, the information provided from the plan, and how the plan is administered to determine whether it has to comply with the HIPAA Privacy Rule and if so, how. Some compliance obligations for a covered plan to consider are described here.

**Privacy officer/training –** Covered entities must designate a privacy officer, along with an employee who will receive complaints, respond to questions about the privacy policy and provide written notice of the privacy practices upon request. Training should be provided to all employees who will be involved with the group health plan.

**Plan documents –** The HIPAA Privacy Rule requires that group plan documents establish the permitted and required uses of Protected Health Information (PHI) by the plan sponsor. These statements must be in place before any PHI can be disclosed. There must also be adequate separation of the group health plan and the plan sponsor. This can be accomplished by identifying the employees or the classes of employees who will have access to protected health information. Access must be restricted and is to be used only for plan administrative functions.

**Notice of privacy practices –** The HIPAA Privacy Rule requires the distribution of a written notice of the covered entity's privacy practices to plan participants (in the case of a health plan) or patients, if the covered entity is a health care provider. A self-insured employee benefit plan that is covered by HIPAA should provide this written notice to plan participants upon request.

This is general information and is

### Covered Entities

Health Plan - an individual or group plan that provides or pays the cost of medical care. Common examples of "health plans" include:

- An ERISA group health plan (providing medical care) if the plan has 50 or more participants or is not self-administered by the employer
- An issuer of health insurance
- An issuer of long term care insurance
- An HMO
- Medicare Part A or Part B
- Medicaid
- An issuer of a Medicare supplemental policy
- A multiple employer welfare benefit plan
- Other individual or group plans that provide or pay the cost of medical care

only intended to give you a basic understanding of how the HIPAA rules may apply to self-insured plans. For professional advice specific to your situation, please consult your attorney.

### *Individual Rights*

Under the HIPAA Privacy Rule, every individual is entitled to receive a notice of privacy practices from his or her health plan, health care provider or health care clearinghouse. An individual also has the right to access certain protected health information and request that changes be made. Under certain circumstances, a covered entity must maintain and provide an accounting of certain disclosures of protected health information. The HIPAA notice of privacy practices must describe the individual's rights, including the right to complain to the Department of Health and Human Services (DHHS) if they believe their privacy rights have been violated. A point of contact must be included in the notice.

### *Federal, Civil and Criminal Penalties*

The DHHS is responsible for enforcement of the Privacy Rule, and will also provide technical assistance to help covered entities comply with the rule. DHHS can impose civil money penalties of up to $100 per violation, with a maximum of $25,000 for multiple violations of the same rule requirement. Exceptions include violations that are due to reasonable cause and did not involve willful neglect and those that were corrected within 30 days.

Criminal penalties of up to $50,000 and/or one year in prison can be imposed when a person knowingly and wrongfully obtains or discloses individually identifiable health information. If this offense is committed under false pretenses, penalties can reach $100,000, up to five years in prison, or both. If the offense is committed with the intent to sell or use the information for commercial advantages, personal gain or malicious harm, a penalty of up to $250,000 and/or up to 10 years in prison may be imposed. Criminal penalties will be enforced by the Department of Justice.

## UnumProvident's Compliance with HIPAA

UnumProvident has reviewed the HIPAA law and related final regulations to ensure full and timely compliance of UnumProvident's systems and procedures with applicable HIPAA requirements.

### *Privacy*

UnumProvident has reviewed the Standards for Privacy of Individually Identifiable Health Information promulgated by the Department of Health and Human Services (HHS) pursuant to HIPAA and is complying with these regulations for impacted products. Most health plans that are covered by the regulations were required to comply with the new requirements by April 14, 2003.

Please note that the majority of UnumProvident's products are exempt from HIPAA mandates. For example, long term disability, short term disability, life, supplemental disability, accident and critical illness coverages are excluded from HIPAA privacy regulations. However, certain products are covered, including long term care and various "medical" plans such as cancer policies (hereafter, "covered products").

For long term care and other products covered under the HIPAA privacy regulations, UnumProvident has amended numerous service provider (business associate) contracts, developed and distributed privacy notices to covered policyholders, and revised our application and claim authorizations for those products impacted by the privacy regulations. We are also using HIPAA authorizations during our underwriting and claims processes for products not covered by HIPAA to facilitate collection of health information from health care providers who are covered by HIPAA.

### *Security*

UnumProvident is in the process of enhancing our Enterprise Security Framework. This will provide UnumProvident with a unified security framework that will provide the direction to ensure the availability, integrity and accuracy of company assets, customer data and personally identifiable information. The framework will provide the foundation that enables secure access to company assets by employees, customers and business partners any time from anywhere. Components include, but are not limited to:

- Security policies, procedures and guidelines
- Security awareness and training
- Risk assessment and management
- Data classification
- Security monitoring and reporting
- Incident response/management
- Security consulting
- Security auditing
- Implementation/utilization of the security tools of the trade.

UnumProvident is using the Information Security Standards of the ISO 17799 as well as HIPAA security requirements as guides to the development of this framework. Our goal is to be in compliance with these standards by the compliance date of April 21, 2005.

### *Electronic Data Interchange*

Federal regulations adopted under HIPAA establish "Standard Transactions and Code Sets" for the sharing of certain data by electronic means. These standards for data elements, code sets and formats are to be used by certain entities (covered entities) when those entities use electronic data interchange to conduct certain transactions (covered transactions) for insurance products that are covered by HIPAA (covered products). **Covered entities** include certain insurers to the extent their insurance products are covered products. **Covered transactions** are certain HHS defined electronic transfers of information to carry out financial or administrative activities related to covered products.

UnumProvident has undertaken an extensive review and inventory of its products and data transfers to verify those that are within the scope of the HIPAA definitions. We have developed policies and procedures so that UnumProvident is capable of conducting covered transactions with respect to our covered products using the mandated Standard Transactions and Code Sets.

# Appendix

## Covered Entity Document

Following is a redacted version of 42 U.S.C. 1395x(s):

42 U.S.C. 1395x(s) Medical and other health services.

The term ''medical and other health services" means any of the following items or services:

(1) physicians' services;
(2) (A) services and supplies (including drugs and biologicals which are not usually self-administered by the patient) furnished as an incident to a physician's professional service, of kinds which are commonly furnished in physicians' offices and are commonly either rendered without charge or included in the physicians' bills;
(B) hospital services (including drugs and biologicals which are not usually self-administered by the patient) incident to physicians' services rendered to outpatients and partial hospitalization services incident to such services;
(C) diagnostic services which are -
i. furnished to an individual as an outpatient by a hospital or by others under arrangements with them made by a hospital, and
ii. ordinarily furnished by such hospital (or by others under such arrangements) to its outpatients for the purpose of diagnostic study;
(D) outpatient physical therapy services and outpatient occupational therapy services;
(E) rural health clinic services and federally qualified health center services;
(F) home dialysis supplies and equipment, self-care home dialysis support services, and institutional dialysis services and supplies;
(G) antigens (subject to quantity limitations prescribed in regulations by the Secretary) prepared by a physician, as defined in subsection (r)(1) of this section, for a particular patient, including antigens so prepared which are forwarded to another qualified person (including a rural health clinic) for administration to such patient, from time to time, by or under the supervision of another such physician;
(H) i. services furnished pursuant to a risk-sharing contract to a member of an eligible organization by a physician assistant or by a nurse practitioner and such services and supplies furnished as an incident to his service to such a member as would otherwise be covered under this part if furnished by a physician or as an incident to a physician's service; and
ii. services furnished pursuant to a risk-sharing contract to a member of an eligible organization by a clinical psychologist (as defined by the Secretary) or by a clinical social worker, and such services and supplies furnished as an incident to such clinical psychologist's services or clinical social worker's services to such a member as would otherwise be covered under this part if furnished by a physician or as an incident to a physician's service;
(I) blood clotting factors, for hemophilia patients competent to use such factors to control bleeding without medical or other supervision, and items related to the administration of such factors, subject to utilization controls deemed necessary by the Secretary for the efficient use of such factors;
(J) prescription drugs used in immunosuppressive therapy furnished, to an individual who receives an organ transplant for which payment is made under this subchapter;
(K) i. services which would be physicians' services if furnished by a physician and which are performed by a physician assistant under the supervision of a physician and which the physician assistant is legally authorized to perform by the state in which the services are performed, and such services and supplies furnished as incident to such services as would be covered under subparagraph (A) if furnished incident to a physician's professional service; but only if no facility or other provider charges or is paid any amounts with respect to the furnishing of such services, and
ii. services which would be physicians' services if furnished by a physician and which are performed by a nurse practitioner or clinical nurse specialist working in collaboration with a physician which the nurse practitioner or clinical nurse specialist is legally authorized to perform by the state in which the services are performed, and such services and supplies furnished as an incident to such services as would be covered under subparagraph (A) if furnished incident to a physician's professional service, but only if no facility or other provider charges or is paid any amounts with respect to the furnishing of such services;
(L) certified nurse-midwife services;
(M) qualified psychologist services;
(N) clinical social worker services;
(O) erythropoietin for dialysis patients competent to use such drug without medical or other supervision with respect to the administration of such drug, subject to methods and standards established by the Secretary by regulation for the safe and effective use of such drug, and items related to the administration of such drug;
(P) prostate cancer screening tests;
(Q) an oral drug (which is approved by the Federal Food and Drug Administration) prescribed for use as an anticancer chemotherapeutic agent for a given indication, and containing an active ingredient (or ingredients), which is the same indication and active ingredient (or ingredients) as a drug which the carrier determines would be covered pursuant to subparagraph (A) or (B) if the drug could not be self-administered;
(R) colorectal cancer screening tests; and
(S) diabetes outpatient self-management training services;
(T) an oral drug (which is approved by the Federal Food and Drug Administration) prescribed for use as an acute anti-emetic used as part of an anticancer chemothera-

peutic regimen if the drug is administered by a physician (or as prescribed by a physician) -
i. for use immediately before, at, or within 48 hours after the time of the administration of the anticancer chemotherapeutic agent; and
ii. as a full replacement for the anti-emetic therapy which would otherwise be administered intravenously;

(U) screening for glaucoma for individuals determined to be at high risk for glaucoma, individuals with a family history of glaucoma and individuals with diabetes; and

(V) medical nutrition therapy services in the case of a beneficiary with diabetes or a renal disease who -
i. has not received diabetes outpatient self-management training services within a time period determined by the Secretary;
ii. is not receiving maintenance dialysis for which payment is made under Medicare; and
iii. meets such other criteria determined by the Secretary after consideration of protocols established by dietitian or nutrition professional organizations;

(3) diagnostic X-ray tests (including tests under the supervision of a physician, furnished in a place of residence used as the patient's home, if the performance of such tests meets such conditions relating to health and safety as the Secretary may find necessary and including diagnostic mammography if conducted by a facility that has a certificate (or provisional certificate) issued under section 354 of the Public Health Service Act, diagnostic laboratory tests, and other diagnostic tests;

(4) X-ray, radium, and radioactive isotope therapy, including materials and services of technicians;

(5) sugical dressings, and splints, casts, and other devices used for reduction of fractures and dislocations;

(6) durable medical equipment;

(7) ambulance service where the use of other methods of transportation is contraindicated by the individual's condition, but only to the extent provided in regulations;

(8) prosthetic devices (other than dental) which replace all or part of an internal body organ (including colostomy bags and supplies directly related to colostomy care), including replacement of such devices, and including one pair of conventional eyeglasses or contact lenses furnished subsequent to each cataract surgery with insertion of an intraocular lens;

(9) leg, arm, back, and neck braces, and artificial legs, arms, and eyes, including replacements if required because of a change in the patient's physical condition;

(10) (A) pneumococcal vaccine and its administration and, subject to section 4071(b) of the Omnibus Budget Reconciliation Act of 1987, influenza vaccine and its administration; and

(B) hepatitis B vaccine and its administration, furnished to an individual who is at high or intermediate risk of contracting hepatitis B (as determined by the Secretary under regulations);

(11) services of a certified registered nurse anesthetist;

(12) subject to section 4072(e) of the Omnibus Budget Reconciliation Act of 1987, extra-depth shoes with inserts or custom molded shoes with inserts for an individual with diabetes, if -

(A) the physician who is managing the individual's diabetic condition
i. documents that the individual has peripheral neuropathy with evidence of callus formation, a history of pre-ulcerative calluses, a history of previous ulceration, foot deformity, or previous amputation, or poor circulation, and
ii. certifies that the individual needs such shoes under a comprehensive plan of care related to the individual's diabetic condition;

(B) the particular type of shoes are prescribed by a podiatrist or other qualified physician; and

(C) the shoes are fitted and furnished by a podiatrist or other qualified individual (such as a pedorthist or orthotist, as established by the Secretary) who is not the physician described in subparagraph (A) (unless the Secretary finds that the physician is the only such qualified individual in the area);

(13) screening mammography;

(14) screening pap smear and screening pelvic exam; and

(15) bone mass measurement.

No diagnostic tests performed in any laboratory, including a laboratory that is part of a rural health clinic, or a hospital shall be included within paragraph (3) unless such laboratory -

(16) if situated in any state in which state or applicable local law provides for licensing of establishments of this nature,

(A) is licensed pursuant to such law, or

(B) is approved, by the agency of such state or locality responsible for licensing establishments of this nature, as meeting the standards established for such licensing; and

(17) (A) meets the certification requirements under section 353 of the Public Health Service Act; and

(B) meets such other conditions relating to the health and safety of individuals with respect to whom such tests are performed as the Secretary may find necessary.

There shall be excluded from the diagnostic services specfied in paragraph (2)(C) any item or service [except services referred to in paragraph (1)] which would not be included under subsection (b) of this section if it were furnished to an inpatient of a hospital. None of the items and services referred to in the preceding paragraphs [other than paragraphs (1) and (2)(A)] of this subsection which are furnished to a patient of an institution which meets the definition of a hospital shall be included unless such other conditions are met as the Secretary may find necessary relating to health and safety of individuals with respect to whom such items and services are furnished.

[1] www.consumer.gov/iditheft/, ID Theft website maintained by the Federal Trade Commission. March 2003.

[2] "Stolen Identity," HR Magazine, January 10, 2003.

[3] Federal Trade Commission. www.consumer.gov/sentinel. March 2003.

[4] TransUnion, Fraud Victim Assistance Department Information Kit, www.transunion.com, September 2003.

[5] International Association for Human Resource Information Management, Privacy & Security Special Interest Group. http"//www.privacy-security-sig.org. March 2003.

[6] The National Association of Insurance Commissioners (NAIC), an organization of insurance regulators from the 50 states, the District of Columbia and the four U.S. territories, was formed in 1871 to address the need to coordinate regulation of multi-state insurers. The NAIC now provides a forum for the development of policy that protects the interests of insurance consumers.

[7] Examples are taken from the section 4(k) provisions and regulations on financial activities, found on the FTC's website, www.ftc.gov/privacy/glbact/indes.html. March 2003.

[8] As Part of "Operation Detect Pretext" FTC Sues to Halt Pretexting, Federal Trade Commission, April 2001. www.ftc.gov.

[9] Summary of the HIPAA Privacy Rule, United States Department of Health and Human Services, Office for Civil Rights, Revised May 2003.



UnumProvident Corporation
1 Fountain Square, Chattanooga, TN 37402
2211 Congress Street, Portland, ME 04122
www.unumprovident.com



G-73608 (1-04)