INSURANCE CONTINUING EDUCATION

MAJOR ISSUES IN INSURANCE

STATE-APPROVED CONTINUING EDUCATION
for
CALIFORNIA INSURANCE LICENSEES

BOOKMARKEDUCATION

BookmarkEducation.com
(800) 716-4113

MAJOR ISSUES IN INSURANCE

California Approved Course License Number 319051

A considerable amount of care has been taken to provide accurate and timely information. However, any ideas, suggestions, opinions, or general knowledge presented in this text are those of the authors and other contributors, and are subject to local, state and federal laws and regulations, court cases, and any revisions of the same. The reader is encouraged to consult legal counsel concerning any points of law. This book should not be used as an alternative to competent legal counsel.

Printed in the United States of America.
▪P3▪

All inquiries should be addressed to:

Bookmark Education
6203 W. Howard Street
Niles, IL 60714
(800) 716-4113
BookmarkEducation.com

CHAPTER 1: ANTI-TERRORISM EFFORTS IN INSURANCE 1

Introduction 1
Terrorism and the Insurance Industry: Pre-9/11 1
The Attacks and the Initial Response 2
Insurers Feel the Fiscal Pain 2
A Coverage Crisis Begins 3
Businesses Ponder Life Without Coverage 4
Documented Effects of Exclusions and Decreased Availability 4
Terrorism and Workers Compensation 5
Protecting Insurers Through TRIA 5
Protecting the Public Through Anti-Money Laundering Programs 6
What Is Money Laundering? 6
How Criminals Commit Money Laundering 7
Cooperating With Foreign Entities 7
Major Money Laundering Cases in Insurance 8
The USA Patriot Act 8
The Bank Secrecy Act 9
Role of FinCen 10
Covered Insurance Products 10
Non-Covered Products 11
Anti-Money Laundering Programs 12
Compliance for Variable Insurance Products 14
Mandatory Producer/Employee Training 14
Suspicious Activity Reports 15
Reporting Large Transactions 16
Conclusion 16

CHAPTER 2: INSURANCE DISCRIMINATION - THEN AND NOW 16

Introduction 16
Racial Issues in Insurance 17
Redlining 18
Disabilities and Pre-Existing Conditions 20
The Health Insurance Portability and Accountability Act 21
The Affordable Care Act 24
Mental Health Parity 25
Genetic Information 25
The Genetic Information Non-Discrimination Act 26
Gender Discrimination 27
Insurance Discrimination Against Men 27
Insurance Discrimination Against Women 27
Domestic Abuse 29
Marriage Discrimination 29
Sexual Orientation 30
HIV/AIDS 30
Credit Scoring 31
Age 32
Dog Breed 32
Travel Plans 33
Conclusion 33

CHAPTER 3: HIPAA PRIVACY COMPLIANCE 33

Introduction 33
General Overview of HIPAA 33
A Disclaimer About This Chapter 34
Health Information Privacy Rules 34
Kinds of Protected Health Information 34
Applicability to Covered Entities 36
Applicability to Employees 38
Applicability to Business Associates 38
Applicability to Plan Sponsors 40
Parties Exempt From the Privacy Rule 40
Required Authorization and Consent Forms 41
Permissible Use and Sharing of Protected Health Information 42
Right to Your Own Information 45
Accountings of Disclosures 47
Rights of Your Personal Representative 47
Sharing Information in an Emergency 48
Sharing Information in the Workplace 50
Using Information for Marketing Purposes 52
Sharing Information With the Government, the Courts and Other Authorities 52
Other Assorted Privacy Requirements 53
Relationship to Other Privacy Laws 54
Health Information Security Rules 54
Implementing a Security Plan 54
Required Safeguards and Addressable Safeguards 55
Dealing With Security Breaches 57
Criminal and Civil Penalties 59
Conclusion 59

CHAPTER 4: ERRORS, OMISSIONS AND PROFESSIONAL LIABILITY 59

Introduction..... 59
Liability Risks for Insurance Professionals 59
Liability and the Producer-Consumer Relationship..... 60
The Need for Professional Liability Insurance . 61
Aren't Professionals Already Covered? 61
Obtaining Professional Liability Insurance..... 62
An Assortment of Policies..... 62
Errors and Omissions Insurance and Malpractice Insurance 62
Who is Covered Under an Errors and Omissions or Malpractice Policy?..... 64
Package Deals 64
Employment Practices Liability Insurance .. 64
Fiduciary Liability Insurance 65
Deductibles and Co-Payments..... 65
Benefit Limits..... 66
Towers of Coverage 66
Liability Premiums 66
Claims-Made Policies and Occurrence Policies67
Pros and Cons of Occurrence Policies 67
Media Liability Insurance 68
Reporting Liability Claims..... 68
Prior Acts..... 68
Nose Coverage..... 68
Tail Coverage 69
Defense Costs..... 69
Duty to Defend..... 70
Timing of Defense Benefits..... 70
Reservation of Rights 71
Settlements 71
Hammer Clauses..... 71
Policy Exclusions..... 72
Coverage Under Other Polices..... 72
Insured vs. Insured Exclusion..... 72
Pollution Exclusions..... 72
Other Exclusions 73
Policy Rescissions and Severability 73
Conclusion..... 74

CHAPTER 1: ANTI-TERRORISM EFFORTS IN INSURANCE

Introduction

Whether they want to or not, today's insurance professionals need to consider how the threat of domestic or international terrorism might impact their business. The potential damage brought on by suicide bombers and other violent extremists can produce significant losses in practically all lines of insurance. Meanwhile, some members of the insurance community are legally required to be especially vigilant and help the federal government uncover suspicious financial activities.

The first main section of this material will provide a historical perspective on the industry's reaction to the September 11, 2001, terrorist attacks. Later, you will read about some of the compliance-related measures that were implemented in response to those events, including requirements for producers and carriers to help keep us safe.

Terrorism and the Insurance Industry: Pre-9/11

Prior to September 11, 2001, few Americans outside of the airline industry concerned themselves with obtaining terrorism risk insurance. If average citizens worried about the issue at all, they usually confined their thoughts to the effects of terrorism on overseas vacations. A pricey trip to London, for example, could have become even more costly for the traveler if unrest regarding Northern Ireland prompted someone to set off bombs in the city, forced the cancellation of commercial flights and indefinitely stranded the tourist a long way from home.

The cautious American could have guarded against such hypothetical disasters by purchasing a policy like the one Access America introduced in 1986, according to the Boston Globe, which covered losses sustained as a result of foreign terrorism at a cost of $3 to $7 for each travel day.

In retrospect, however, even that rare example of a pre-September 11 terrorism-related insurance product hints at the era's treatment of terror as a largely implausible threat to U.S. citizens. The terrorism aspect of the policy snared some modest media attention for its parent company, but, in reality, the coverage represented only one element of a multi-faceted product that also insured against emergency hospitalization (terrorism-related or otherwise), lost luggage and other potential hassles for globetrotters.

Until 9/11, even major domestic insurance companies didn't seem to be giving a significant amount of thought to the level of terrorism risk in the United States. Standard policies from property insurers shielded carriers from having to cover most losses caused by war, but the language of these war exclusions generally wasn't specific enough to be enforceable after an attack from someone other than a foreign government (such as an independent terrorist organization).

This relatively soft approach to terrorism-related insurance issues continued even as the United States found itself in violent situations during the last quarter of the twentieth century. When suspected Libyan bombings in West Berlin prompted U.S. retaliation in 1986, Libyan leader Muammar al-Qaddafi vowed revenge. Although Qaddafi's threats provoked an increase in the cost of terrorism insurance for the airline industry, insurers didn't alter their treatment of coverage for commercial properties on American soil.

When four men set off a car bomb underneath the World Trade Center seven years later, killing six people and injuring 100, neither insurers nor lawmakers put forth a resolute effort in an effort to confront terrorism-related risks. Then, in 1995, domestic terrorists bombed a federal building in Oklahoma City, killing more than 100 people and injuring more than 400. At that time, some insurers wondered out loud about their business's approach to terrorism, but the industry never progressed beyond the talking stage to the point of implementing widespread exclusions of such risks.

Those worries about terrorism on the home front had faded, for the most part, by early September 2001, with insurers experiencing a modestly decent period in their business cycle following years of soft markets but generally adequate profits. According to the U.S. Treasury's June 30, 2005, report on terrorism risk insurance, property and casualty insurers had earned either increased or steady levels of surplus between 1994 and 2000.

The terrorist attacks on the World Trade Center and the Pentagon changed all of that by offering indisputable proof of America's vulnerability to acts of mass destruction. At their most human level, the events of September 11 altered Americans' perception of their place in an often dangerous world. The country proved strong enough to withstand horrific threats on its livelihood, but a logical observer could no longer argue that the United States was somehow protected from outside enemies by an invisible shield of military strength and international influence. America learned the hard way that the risks involved with terrorism required greater vigilance and preparation than had previously been expected. The time had come for the insurance community to consider scary scenarios that were once unthinkable.

The Attacks and the Initial Response

The September 11 attacks on the United States killed approximately 3,000 people, injured several thousands more and resulted in damage that was initially estimated to be anywhere from $25 billion to $70 billion. Despite the fact that national security reigned over the minds of most Americans during the days that followed, the nation's business community forced itself to ponder who would shoulder the financial burden of the costliest disaster in U.S. history up to that point. Although the shocking, catastrophic nature of the situation showed exactly why a person or business should purchase insurance, even policyholders with extensive coverage had a reason to nervously hold their breath in anticipation of an industry-wide response.

Traditionally, insurance companies can exempt themselves from having to pay certain insurance claims following acts of war. A massive conflict on domestic soil, after all, could potentially bankrupt the issuer. Although many life insurance providers omitted these exclusions from their policies after the Vietnam War, they still appear in many property and casualty insurance products.

The violent, politically motivated attacks of September 11 certainly seemed warlike at first. In speech after speech, President George W. Bush and members of his administration used the phrase "act of war" to describe al-Qaeda's hijacking and subsequent crashing of four U.S. planes. Legal definitions of "acts of war," though, usually contained references to nations. Regardless of the United States' eventual invasion of Afghanistan in response to the Taliban regime's support of al-Qaeda, the September 11 attacks were technically carried out by an independent, internationally organized terrorist group and not by a specific government.

These factors presented the insurance industry with a few very difficult choices. It could have ignored the act of war exclusions and made huge payments to policyholders, or it could have invoked the war exclusions and risked being overruled by the government and/or disdained by a hurting public.

The only good news for insurers was that they had incorrectly counted on experiencing heavy seasons of earthquakes and hurricanes in the several months preceding the attacks. Mother Nature spared the United States somewhat from natural disasters during that time, spoiling insurers' expectations but leaving them with enough money to handle some other form of trouble.

Ultimately, within days of the terrorist acts, the industry representatives announced their intention to pay all legitimate insurance claims that were caused by al-Qaeda's assaults without invoking exclusions for acts of war. While cheered by business observers in the moment, the decision turned out to be a response specifically to the 9/11 attacks and not at all a promise to cover similar losses in the event of future strikes. It was only a matter of time before a more permanent solution to terrorism risk would be needed in order to keep insurers and the economy stable.

Insurers Feel the Fiscal Pain

Of all the disasters ever experienced in the United States up to that time, the events of September 11 affected the broadest range of insurers. The financial repercussions of the attacks bruised even the era's most fiscally strong carriers, while exposing the mismanagement and instability of weaker companies.

At the time of the attacks on the World Trade Center and the Pentagon, General Re Corp. was the fourth-largest reinsurer in the world, helping major insurance companies obtain insurance to manage their own risks. Under the guidance of investor Warren Buffett, General Re's parent company, Berkshire Hathaway, had increased its net worth for 37 consecutive years. September 11 cost Berkshire Hathaway roughly $2.28 billion, with most of that total resulting from the insurance end of its business.

Assessing his company's preparedness in regard to terrorism, Buffett claimed General Re could perhaps withstand another attack similar to those on the World Trade Center and the Pentagon but that anything larger or more sophisticated in its weaponry could seriously disable his business. Buffett frighteningly envisioned a future in which terrorists would move beyond the use of airplanes and bombs and toward nuclear, chemical and biological weapons that could destroy enormous amounts of properties and human lives.

With those concerns on his mind, Buffett said General Re would be incapable of covering losses from chemical or biological warfare and that coverage for nuclear-related losses would be an expensive rarity for his reinsurance customers. The company also began paying greater attention to the potential risk of highly concentrated properties by putting stricter limits on the number of structures it insured within the same geographic area. Buffett addressed his industry's old-school approach to terrorism, pointed a finger at himself and said failing to charge consumers an extra amount for coverage of terrorism losses was a huge mistake.

But General Re still stood firmly on its two legs after September 11 and could look forward to a profit-making phase brought on by price increases and people's general cravings for insurance following a catastrophic event. Other companies weren't so lucky.

By September 2002, two reinsurance companies had reached a state of insolvency and ceased writing new business as a result of al-Qaeda's suicide missions. The demise of Copenhagen Re was a relatively straightforward case of policy risks coming to life and proving too costly for the carrier to handle. Many of the reinsurer's best and brightest employees had left the organization years earlier, and its premiums and reserves seemed uncomfortably low compared to industry norms during the pre-September 11 business cycle.

North Carolina-based Fortress Re's tale, however, as reported by Mark Maremont in a series of articles for the Wall Street Journal, detailed a multi-faceted mess of questionable accounting and ethics. Employed as a U.S. agent for Sompo Japan Insurance Corp., Fortress became a visible force in aviation reinsurance. The company sold policies that covered anywhere between the first $50 million to $400 million of damages from a crash. Those risky plans made Sompo liable if nearly any of its insured planes went down. In order to reduce its risk, Sompo instructed Fortress to purchase reinsurance that would reduce the parent organization's liability. Fortress received one-third of any profits, minus the cost of the reinsurance.

Following the four hijackings on September 11, all of which occurred on planes that were insured by Sompo, Fortress finally surrendered its well-guarded books to its overseas bosses. In fact, Fortress had not purchased traditional reinsurance that allowed Sompo to share risks with other parties. Instead, the agent had opted for cheap finite reinsurance. Via that arrangement, Sompo received immediate financial assistance from its reinsurers when paying claims, but the Japanese company was required to pay the money back with interest over a number of years. By purchasing less-expensive finite insurance instead of traditional reinsurance and by allegedly failing to alert its superiors to the financial commitments involved with the policies, Fortress Re, according to an eventual lawsuit, falsified its profits and thus allegedly received higher commissions from Sompo than it deserved.

In the end, the combination of Fortress's alleged actions and the September 11 attacks caused Taisei Fire, one part of the Sompo empire, to become just the second Japanese casualty insurance company to file for bankruptcy protection since World War II, and Sompo reported a loss of $1.4 billion as a result of September 11.

These examples of instability in the reinsurance market meant that traditional insurance companies would struggle to obtain insurance for themselves. And without the ability to manage their own risks with confidence, those carriers (it was ultimately assumed) would need to make up for their uncertainty by charging more or making coverage unavailable in the usual insurance market.

A Coverage Crisis Begins

These examples of major losses help explain why, in late September 2001, spokespeople for the insurance industry announced to the U.S. House Financial Services Committee that carriers planned to exclude terrorism coverage from standard property and casualty policies beginning in January of 2002. Reinsurers

(which essentially provide insurance for insurance companies) didn't want to share in the risks, and insurers didn't want to keep the risks for themselves.

Many state insurance regulators sat on the issue at first and waited for the federal government to address the problem. When that did not happen by December 31, 2001, (when 70 percent of U.S. property and casualty policies were due to expire), the terrorism coverage exclusions went into effect in 45 states. New York, California, Georgia, Florida and Texas were the only states that denied insurers' requests to exclude terrorism risks.

The exclusions added in 2002 didn't wipe out all coverage for terrorism-related losses, but they gave insurers flexibility. Some small insurers still offered free coverage, but those instances were relegated to low-risk policyholders. A shoe store in Beaufort, South Carolina, for example, might have been eligible for terrorism insurance at no additional cost, but an office building in the heart of Boston almost certainly had to pay for it.

Metropolitan businesses watched their premiums soar thanks to insurers' new attitude toward terrorism. Chicago's chief financial officer Walter Knorr reported that the city spent $125,000 in 2001 for $750 million in terrorism-related coverage for its airports. After September 11, the same insurer charged $7 million for $150 million of protection.

Businesses Ponder Life Without Coverage

Had the events of September 11 not occurred, exclusions of terrorism in insurance policies might not have produced much major concern among various sectors of the business world. But with al-Qaeda's attacks fresh in everyone's minds, many people—whether they were buyers and sellers of real estate, mortgage lenders or investors—became extremely reluctant to make major financial commitments to projects that weren't fully insurable.

As the December 31, 2001, date for renewals of most commercial property and casualty policies approached, the business community faced an undesirable future without affordable terrorism protection. Most lenders required nearly all-risk insurance for loans above $50 million, and if a property owner lacked insurance against terrorism, lenders could claim that the borrower was in violation of the terms of mortgage agreements and could call for repayment of existing loans.

Without the insurance, businesses worried that new loans would be denied and that developers would be forced to stop building trophy properties that might seem like obvious targets for terrorists. Widespread downturns in the real estate industry would inevitably affect the national economy. According to a late 2001 report by the Mortgage Bankers Association, the real estate trade produced 12 percent of the year's gross domestic product and employed 8.5 million people. Those figures included not only brokers and salespersons in real estate but also workers in the construction industry, who would lose jobs if there was nothing to build.

Some in the real estate and mortgage industries predicted that a company's inability to obtain terrorism risk insurance on a particular property would force the business to relocate. Although that possibility might have helped less densely populated areas of the country by bringing jobs and economic growth to different communities, people generally agreed that high concentrations of businesses in major cities aided efficiency and competition.

Documented Effects of Exclusions and Decreased Availability

In some cases, the fears surrounding the unavailability terrorism insurance for terrorism-related losses were proven valid by real problems that surfaced in 2002. In other cases, what actually occurred in the business world weren't in line with some of the initial worries. Under the circumstances, many insureds got creative with their coverage and did their best to adjust to a rapidly hardening market.

A number of property owners dealt with high prices by insuring their entire real estate portfolio at a low level. Owners calculated that, in this way, they could survive an attack financially if each of their buildings was at least partially covered. Some companies opted to spread out and open smaller offices instead of containing every aspect of their business within a single skyscraper. However, lack of coverage didn't force a massive

exodus by businesses away from cities like New York and Chicago to areas of the country where the terrorism risk seemed lower.

Some banks didn't pull back loans from uninsured borrowers, but they asked for higher rates of return on their loans. Other lenders exempted small businesses from all-risk requirements unless a business was situated near a high-risk property. Assorted lenders financed initially uninsured projects but insisted that property owners eventually seek out affordable terrorism coverage.

The relatively small amount of specific, reported horror stories related to terrorism insurance probably made some people wonder if real estate professionals and lenders were blowing the issue out of proportion, but on a broader scope, some numbers supported claims of a crisis. GMAC announced in June 2002 that it had rejected $1 billion in loan requests because applicants didn't possess adequate terrorism coverage. A 2002 survey conducted by the Real Estate Round Table found that deals of $15.5 billion in 17 states had been postponed or revoked due to the missing insurance.

Terrorism and Workers Compensation

Businesses that managed to avoid problems related to real estate still had to address terrorism coverage through their workers compensation plans. With some exceptions for certain industries and small businesses, employers in almost every state must monetarily compensate employees who are injured or become ill while performing job-related activities. The September 11 terrorist attacks resulted in $3 billion to $5 billion in workers compensation claims. These collective claims involved deaths and physical injuries along with many cases of serious stress disorders.

Regulators in 45 states generally allowed insurers to exclude terrorism coverage from most property and casualty policies, but they didn't necessarily allow carriers to extend that exclusion to workers compensation insurance. Reinsurers, on the other hand, had the power to exclude this coverage and ultimately left the insurance companies with an undesirable choice between raising prices for commercial policyholders or not doing business with certain employers at all.

Terrorism risk insurance for workers compensation wasn't as difficult to find as similar coverage for commercial property. In an act of last resort, employers could obtain coverage through state high-risk pools. But businesses hoping to get good deals for workers compensation couldn't avoid high prices in either the traditional or nontraditional markets.

Fearing attacks similar to September 11, insurers that offered workers compensation coverage began collecting more extensive information about their current and potential clients. They started to care less about the nature of a company's business and more about that company's office space and number of employees. Organizations that occupied several floors in skyscrapers and employed hundreds of workers at the same location sometimes struggled to obtain terrorism risk coverage. In some cases, businesses requested insurance from 30 carriers and received only one quote in response.

Protecting Insurers Through TRIA

In an effort to keep the economy moving and ensure that terrorism risk insurance was available, Congress passed the Terrorism Risk Insurance Act of 2002 (TRIA). Among other things, this law created a federal backstop for insurers that can be utilized if insured losses from a terrorist attack ever exceed certain dollar amounts (generally several billions of dollars). ‘

In return for this federal help, insurers in the United States are generally required to make terrorism coverage available to applicants for most kinds of property and casualty insurance intended for businesses.. Be aware that although insurers generally must offer insurance against terrorism risk to businesses, an insurer can charge an extra amount for it, and a business can decline the coverage by signing the appropriate form.

Even before TRIA was introduced in Congress, the federal government's role in stabilizing the market for terrorism coverage was a matter of fierce debate. Supporters of the law generally believed that the potential for economic uncertainty was too great for the government to do nothing. They also often claimed that the government had a responsibility to help insurers manage terrorism risks because terrorist activities are often committed in response to a government's foreign policy decisions. On the other hand, critics of a federal

backstop have been concerned about the government potentially taking on too much financial liability and interfering with the free market.

Those points of view were continued to compete with one another in the years after TRIA was passed. After being extended multiple times, the provisions of TRIA actually expired at the end of 2014. However, as they had in the past, insurance trade associations successfully convinced lawmakers to reinstate and extend the law through 2020. Later, the law was extended again through 2027.

Protecting the Public Through Anti-Money Laundering Programs

Considering all the human and financial losses caused by the events of 9/11, it makes sense for insurance professionals to support all reasonable precautions that could thwart similar attacks. As a first step in terrorism prevention, concerned individuals should take time to understand how terrorist organizations are financed. This learning process should emphasize not only the common sources of funding but also how that money moves undetected throughout the global financial system.

Many details regarding al-Qaeda's financial history are provided in the federal government's 9/11 Commission Report. Figures in the document are intriguingly contradictory, painting a portrait of an organization that spent relatively little money on specific plots but still required significant resources to survive. According to the report, the entire undertaking of the 9/11 attacks cost al-Qaeda only roughly $400,000, but total annual expenses for the group in the years leading up to 2001 were estimated at $30 million.

Initially, al-Qaeda was assumed to be funded mainly through the personal fortune of its leader and founder, Osama bin Ladin. Between inheritance of his family's successful construction company and an assortment of ownership interests in other profitable companies, bin Ladin was believed to have a fortune near $300 million. Indeed, later projections confirmed that he was a wealthy man. But those early estimates still greatly overestimated his net worth, and, by the start of the 21st century, many of his personal assets had been either frozen or forfeited amid disputes with multiple Middle Eastern governments.

In reality, most of al-Qaeda's operations were funded through a system of charities. While some donors made major contributions with apparent knowledge of where their money was going, others merely gave money to their local places of worship in accordance with their religious duties and weren't aware of its ultimate destination.

Judgment and detection of terrorism-linked charities was complicated, to a certain degree, by the fact that the groups usually weren't merely a front for violent activities and actually did engage in some legitimate humanitarian work. Meanwhile, when the United States or other vigilant nations unearthed clear connections between terrorists and charities, attempts to halt the flow of money were sometimes hindered by noncooperation from certain foreign governments. These factors (along with several others) combined to create opportunities for al-Qaeda to launder money across the globe.

What Is Money Laundering?

According to some reports, the term "money laundering" dates back to the Prohibition era, when organized crime boss Al Capone used laundry service establishments as fronts for alcohol-related business ventures. Historians have questioned the accuracy of those origins, but Capone's use of a cleaning service as a front for illegal activities was ironically appropriate, particularly if we consider a money launder's ultimate goal.

Criminals engage in money laundering in order to hide financial assets that are either obtained through or used in illegal activities. In essence, a launderer attempts to wash away any trace of illegal behavior to the point where neither a financial institution nor a law enforcement agency can tell the difference between the dirty money belonging to a criminal organization and the clean money earned through legitimate business practices.

Money laundering has been committed seemingly throughout history and was originally a way for indebted borrowers to hide money from their creditors. Authorities in the United States started taking the crime more seriously in the 1970s with an expectation that seizing laundered funds would starve various drug cartels. After 9/11, the federal government began hoping that similar anti-money laundering activities could destabilize terrorist organizations.

For the cartels and other sects of organized crime, money laundering is often a way to withdraw profits after illegal activity has already occurred. In the case of terrorist groups, however, the opposite is often true. Instead of using laundering techniques to obtain funds after committing illegal activity, terrorists are likely to use those techniques in order to facilitate illegal activity in the first place. Due to the differences between money laundering by terrorist groups and money laundering by other criminals, money laundering by terrorists is sometimes known as “reverse money laundering” or “money laundering in reverse.”

In total, the International Monetary Fund, has estimated that between $600 billion and $1.5 trillion is laundered throughout the world every year. Those figures amount to roughly 2 percent to 5 percent of global domestic product.

How Criminals Commit Money Laundering

Some money laundering schemes are relatively simple, and others are complex enough to keep skilled law enforcement authorities scratching their heads for years. In most cases, though, the operation goes through three stages, which we will call: “placement,” “layering,” and “integration."

Placement

When a criminal is in the “placement” stage, he or she is trying to introduce dirty money into the regular economy in a manner that arouses minimal suspicion. For instance, a launderer might make bulk cash deposits that include money linked to criminality and money linked to a cash-heavy front business, such as a car wash, dry cleaning service, convenience store, restaurant or liquor store. Particularly in regard to terrorist groups, placement might begin at a completely bogus or semi-legitimate charitable organization. Within an insurance context, placement might occur by purchasing a cash-value insurance policy or annuity with a large sum of cash.

Concerns about the placement stage of money laundering are at least partially responsible for rules requiring many U.S. financial institutions to report cash transactions of $10,000 or more to the federal government. Criminals might work around this requirement by simply breaking down a large cash deposit into smaller amounts that don’t reach the $10,000 threshold.

Layering

In the “layering” stage of money laundering, launderers and their associates attempt to create a financial maze for regulators by wiring money from one account to another or allowing money to pass through several types of financial institutions. The laundered funds might be moved back and forth between foreign or domestic financial companies regardless of any penalties for early withdrawals. For example, a launderer might use an insurance company to layer money by quickly replacing one fixed annuity with another for no legitimate reason. Any surrender charge resulting from the transfer might be dismissed by the launderer as part of the cost of doing business.

To help ensure that their layering doesn’t receive much attention, some launderers have gone so far as to bribe workers at financial institutions. Some have even bought their own banks here or abroad in order to facilitate schemes. Although inappropriate activity by financial insiders is certainly possible at large institutions, launders might be particularly attracted to smaller entities, where irregular account activity is less likely to be flagged by internal safeguards.

Integration

The final stage in the money laundering process is “integration.” At this point, the money is presumed to be untraceable, “cleaned up” and ready to be spent for personal items or to pay for future criminal activity. This stage is sometimes also referred to as the “receiving” stage of money laundering.

Cooperating With Foreign Entities

Though a criminal could certainly launder money solely on American soil, many of the money laundering cases that attract federal attention involve foreign banks, individual foreign clients and foreign businesses.

Offshore banks in places such as Panama and Switzerland have attracted an international clientele eager to avoid various tax penalties in their own countries. One concern regarding these parts of the world is the

anonymity with which a foreign person or business can create offshore accounts. Unlike in the United States, some countries' banking systems don't maintain customer identification records and often pride themselves on the privacy protections available to their native and foreign customers.

Offshore financing of illegal activity can exist on a number of levels. In its simplest form, it might be done by creating a "correspondent account" used by or set up for a legitimate foreign person or business. In a more complicated plan, people might respond to an advertisement in a foreign publication that highlights attorney services for offshore clients. A U.S.-based launderer could rely on one of these attorneys to form a front business in the foreign country with only the lawyer's name on all the paperwork. Dirty money could then be transferred to the offshore front, and, sooner or later, the U.S. entity could ask the foreign front for a loan, which would be granted and paid back with interest, thereby making the illegal funds clean.

The U.S. government continues to pass stricter laws related to bank and wire transfers to and from correspondent accounts and shell companies. In some cases, international pressure has resulted in banking reforms that have reduced some of the potential for money laundering at foreign financial institutions. However, even when the United States pressures or successfully convinces a government to change its financial privacy laws, another country often comes along and meets the small but powerful demand for anonymous transactions and tax havens.

Without the full support of law enforcement agencies in other countries, efforts to minimize money laundering's impact on U.S. citizens require greater vigilance among domestic entities. In fact, as a result of 9/11, rules have been put in place to help prevent money laundering at many of the nation's insurance companies.

Major Money Laundering Cases in Insurance

Despite the federal government's concern regarding the links between money laundering and terrorist groups, most of the documented cases of money laundering in insurance have been perpetrated by drug dealers. In one case, according to the Financial Action Task Force and cited in the Journal of Money Laundering Control, a trafficker converted $80,000 of drug money into a cashiers check and used it to purchase a single-premium, cash-value life insurance policy, only to surrender the policy for its cash value a mere three months later. Perhaps the most striking aspect of the case, according to reports, was that the salesperson who sold the policy had full knowledge of the money's origins. Instead of reporting the applicant to supervisors or police, the producer demanded and received a higher sales commission in exchange for facilitating the transaction.

A similar but more elaborate case of insurance-related money laundering is detailed in multiple issues of the Federal Register and earned the code name "Operation Capstone" from the U.S. Customs Service. According to court documents and interviews cited by the federal government, Columbian cartels took money earned from drug deals in Mexico and the United States and used it to purchase hundreds of life insurance policies in Europe. Policies worth as much as $1.9 million were surrendered after roughly a year in spite of early withdrawal fees that sometimes exceeded 25 percent of the cash value. But, as stated by the government, "The penalties … merely represented a 'business cost' of using the insurance products to launder the illicit narcotics proceeds." While Operation Capstone was still winding down, the government also noted similar plots involving variable annuity products.

The USA Patriot Act

The insurance industry's greater involvement in anti-money laundering activities stemmed from the passage of the USA Patriot Act. Through the law and the rules that followed it, the federal government signaled that any piece of information about potential terrorist activity—no matter how small—had value. And even though the documented examples of money laundering in insurance weren't connected to terrorist groups, regulators weren't interested in waiting for a test case. If there were ways to exploit the financial system in order to hide significant amounts of money, criminals would presumably find them. And one of the best ways to prevent another attack, lawmakers believed, was to fill the holes in the system before they could be exploited.

Title III of the USA Patriot Act contains the International Money Laundering Abatement and Financial Anti-Terrorism Act. This major section of the law, according to the U.S. Department of the Treasury, made the following important changes in regard to money laundering, among other things:

- Encouraged law enforcement, regulators and financial institutions to share more information with one another about suspected terrorism and money laundering.
- Strengthened the ability of the Departments of Justice and Treasury to seize the funds of individuals and businesses in foreign countries.
- Created new rules for verifying the identity of new customers at financial institutions.
- Gave legal protection to businesses and individuals who report suspicious financial activities to the government.
- Prohibited businesses from telling customers about certain government investigations involving suspicious financial activity.
- Required financial institutions (including some insurance companies) to establish anti-money laundering programs.

We will address that last important point in greater detail later in these course materials. However, in order to understand both the requirements for anti-money laundering programs and the reasons for them, it may be helpful to have a bit more background information at our disposal.

The Bank Secrecy Act

The money laundering sections of the Patriot Act were technically amendments to a 1970 law known as the "Bank Secrecy Act" (BSA). The earlier law called on financial institutions to assist law enforcement by keeping detailed account records and by reporting large currency transactions (generally, those exceeding $10,000) to the U.S. Treasury.

Particularly since 9/11, BSA compliance has been a major issue for a wide variety of businesses. A partial list of entities that must follow certain portions of the law appears below:

- Insurance companies.
- Banks.
- Credit unions.
- Thrifts (savings and loan organizations).
- Currency exchanges.
- Broker/dealers selling securities.
- Investment companies.
- Mortgage lenders.
- Casinos.

Although insurance companies had long been included among those who must comply with the Bank Secrecy Act, practical requirements for those companies were relatively minor. According to the Federal Register, the only BSA requirement for insurers throughout most of the law's history was a section calling for financial institutions to report cash transactions of $10,000 or more to the government. Whereas some other business entities had to follow more specific rules that were designed to implement the law, those initial rules didn't apply to insurers.

The BSA amendments in the Patriot Act prompted regulators to finally clarify an insurance company's obligations in regard to the decades-old law. And along with other financial institutions, insurers discovered that many of those obligations related to the careful creation of internal anti-money laundering programs.

BSA Rules for Insurance Companies

Following the passage of major legislation, the government often issues regulations that are intended to explain how the law should be followed in more practical terms. Anti-money laundering regulations that are specific to the insurance industry went into effect at the federal level in May 2006. We will address some of the details of those regulations shortly, but here's a quick summary of them in advance:

- Some insurance companies must implement procedures to detect possible money laundering.
- Some insurance companies must take special measures to verify the identity of their customers.
- Some insurance companies must appoint compliance officers who are charged with overseeing anti-money laundering procedures.
- Some insurance companies must train their employees to detect potential money laundering.
- Some insurance companies must file special reports with the federal government when money laundering is suspected.

The federal BSA rules for insurers have filled in some of the gaps in parts of the country that lacked their own anti-money laundering rules. When the regulations were originally proposed, according to the National Association of Insurance Commissioners, 12 states didn't have any anti-money laundering requirements for insurers, 29 didn't require documentation of large cash transactions, and all but one didn't specifically require insurers to report possible money laundering to authorities.

In the event that you are legally responsible for anti-money laundering compliance at an insurance company, please be aware that these course materials won't mention the specifics of any state-level laws or state-level rules. Similarly, if BSA compliance is part of your job, you should consult with an expert who is familiar with your situation or at least review the current rules on your own. The explanations of BSA rules that are provided here are intended for general purposes and are not meant to be used as legal advice or as a comprehensive set of an insurer's obligations under various anti-money laundering laws.

Role of FinCen

Anti-money laundering enforcement in the United States is overseen by a section of the U.S. Department of the Treasury called the "Financial Crimes Enforcement Network" (FinCEN). FinCEN was created in 1990 in order to fulfill the following purposes:

- Advise the federal government on issues of financial intelligence and financial crimes.
- Maintain databases related to financial intelligence and financial crimes.
- Analyze data in an effort to decipher criminal activity.
- Promote better communication and sharing of relevant financial information among law enforcement entities.
- Coordinate anti-money laundering procedures with the United States and foreign governments.

Although audits of an insurer's anti-money laundering program (and the imposition of any fines) might be handled by other parts of the Treasury department, FinCEN plays an advisory role in the determination of BSA-related penalties. According to experts quoted in the trade publication Rough Notes, FinCEN might base its disciplinary recommendations on the following factors, among others:

- The amount of money successfully laundered through the company.
- The company's history of compliance (or non-compliance) with BSA requirements.
- The amount of anti-money laundering training conducted by the company for its employees.

Covered Insurance Products

In general, the BSA rules for insurance companies are only applicable to transactions involving "covered products." In choosing which kinds of products would be deemed "covered products," regulators examined the money laundering process and tried to determine the kinds of policy-related features that might attract criminals. Insurance products that can be cancelled in exchange for their cash value are the most likely candidate and are especially vulnerable to laundering when they have free-look periods or modest surrender charges. In short, any insurance product that can easily be converted to real money might be a problem.

Based on those conclusions, the federal government chose to classify the following forms of insurance as "covered products:"

- Permanent life insurance.
- Annuities.
- Any other insurance product with cash value or investment features.

There are many different kinds of permanent life insurance, including whole life, universal life and variable life. The BSA rules define "permanent life insurance" to mean "an agreement that contains a cash value or investment element and that obligates the insurer to indemnify or to confer a benefit upon the insured or beneficiary to the agreement contingent upon the death of the insured."

Many forms of annuities exist, too, including fixed annuities (which offer death benefits along with guarantees of principal and interest) and variable annuities (which might offer some guarantees but are partially dependent on the rise and fall of the stock market). The BSA rules have been applied to both kinds of annuities, with the federal government defining an annuity as "an agreement between the insurer and the contract owner whereby the insurer promises to pay out a fixed or variable income stream for a period of time."

The third group of covered products—essentially anything with cash value or investment features (other than permanent life insurance or an annuity)—was included as a safeguard to ensure that unforeseeable products of the future would still be part of the rules. For example, although FinCEN was unaware of any major property and casualty insurance products that could be exchanged for cash value, it wanted to protect itself in case that hypothetical product ever became a reality.

In commentary from the November 3, 2005, Federal Register, the federal government stressed that there wasn't a minimum dollar amount that would turn a cash-value insurance policy into a non-covered product. However, regulators expect the amount of the cash value to influence an insurer's specific response to a possible suspicious situation. A transaction involving a policy worth $1 million, for instance, might be scrutinized differently than one involving a policy worth only $1,000.

Non-Covered Products

Insurance products without cash values are generally considered to be poor vehicles for money laundering. A scheme in which dirty money is used to purchase real estate (or property insurance) and then laundered by committing property insurance fraud is technically possible but would presumably be much more difficult to complete than the simple purchase and surrender of permanent life insurance.

At the time this course material was being written, several kinds of insurance products were exempt from the majority of BSA requirements, including the rules about anti-money laundering programs. Some of those exempted products are listed below:

- Group life insurance.
- Group annuities.
- Term life insurance.
- Property insurance.
- Casualty insurance.
- Accident and health insurance.
- Reinsurance (essentially, insurance for insurance companies).
- Annuities that are part of a structured workers compensation settlement.
- Credit life insurance.

Insurance companies that do not sell any "covered products" are exempt from the majority of the BSA and its rules. Insurance companies that sell a combination of covered products and non-covered products must abide by the BSA anti-money laundering rules when selling covered products but not necessarily when selling non-covered products.

Be aware that a single product might have characteristics of both a covered product and a non-covered product and that the government has reserved the right to broaden its list of covered products. If your company has questions about whether a particular product must comply with BSA rules, FinCEN can provide a determination for you upon request.

Anti-Money Laundering Programs

An insurance company selling covered products must have an anti-money laundering program that has been reasonably designed to prevent the laundering of money or the funding of terrorism through the organization. The program must be explained in writing and approved by senior management, and a copy of the program must be made available to federal auditors upon request.

In some respects, anti-money laundering programs may be structured in ways that are similar to an insurer's other anti-fraud programs. However, there is usually a difference in the main purpose behind these two types of prevention programs. Whereas anti-fraud programs are generally intended to prevent an insurer from losing money, anti-money laundering programs are meant to serve society as a whole and might help identify illegal activities that don't have a direct impact on an insurer's finances. An early surrender of an annuity, for example, is unlikely to harm the insurance carrier and therefore might not trigger an investigation under the insurer's anti-fraud program. Meanwhile, an anti-money laundering program might flag that scenario as a potentially suspicious activity.

The rules about anti-money laundering programs were intended to be flexible so that they could be implemented at a wide variety of financial institutions. In choosing the particulars of their program, insurance companies are expected to conduct a thorough risk assessment that analyzes their relationship with covered products. Since no two insurance companies are likely to sell exactly the same amount of covered products in exactly the same way, it's possible that no two anti-money laundering programs will be exactly alike.

The federal government requires insurance companies to consider all relevant information as part of creating an anti-money laundering program. According to the Federal Register, factors that should be considered include (but are not limited to) the following:

- Whether the company accepts cash payments for its products.
- Whether the company sells policies in exchange for a single premium or lump sum.
- Whether the company's products allow policyholders to borrow money against their cash value.
- Whether the company accepts business from countries that either sponsor terrorist activities or don't cooperate with U.S. anti-money laundering efforts.

Technically, insurance companies, and not their agents, are required to implement an anti-money laundering program. However, as a condition of their business relationship with a carrier, agents can be ordered to comply with an insurance company's anti-money laundering rules and complete mandatory training.

Knowing Your Customer

In general, BSA rules require financial institutions to develop a "customer identification program." This type of program typically involves confirming the identity of new customers and collecting birthdates, tax identification numbers, names, addresses and more.

Based on the research conducted for this course, experts don't seem to be in total agreement regarding the extent to which insurance companies must implement customer identification programs. However, the federal government has made it clear that insurers must at least collect enough personal information to run an effective anti-money laundering program. Personal information might also need to be collected in order to comply with other federal anti-terrorism laws.

Red Flags of Money Laundering

An insurer's anti-money laundering program will be ineffective (and likely non-compliant with BSA rules) unless the individuals behind it are aware of the "red flags" (or warning signs) of laundering activity. These red flags can relate to the personal responses and behaviors exhibited by individual clients in a question-and-answer session, the products sought by customers, the transactions made by clients and much more.

Although the red flags might be a bit different for each insurer, here are several to be aware of:

- A cash-value product is surrendered at great expense to the owner.
- An owner borrows the maximum amount possible from a cash-value product with policy-loan features.
- An applicant insists on paying large premiums with cash.
- A business has no physical U.S. address (for example, only a P.O. box) and is incorporated in a country that has been known to take a soft approach to anti-money laundering enforcement. (The Financial Action Task Force maintains an up-to-date list of “red flag” countries.)
- Deposits or payments are made in pieces rather than in typical lump sums.
- The owner surrendering a cash-value product has no reasonable explanation for the surrender.
- An applicant displays an unconventionally high amount of interest in policy loans.
- Large purchases are made by people who seem unlikely to afford them (for example, a student buying large amounts of cash-value life insurance).
- Currency used to purchase a product has a strange odor or odd markings.
- The type of product purchased by someone is in conflict with a needs-based analysis conducted by an agent or broker.
- Owners, annuitants or beneficiaries of cash-value products seem unconnected to one another and lack an insurable interest in one another’s lives.
- A consumer asks whether certain transactions must be reported to the Internal Revenue Service.
- Information provided on an insurance application turns out to be false.
- An individual wants to purchase insurance but is very reluctant to provide necessary personal information.
- An applicant wants to purchase an interest-sensitive product but expresses no concern about the product’s performance.
- An expensive insurance product is purchased by someone who has only been in the United States for a very short time and has no reasonable explanation for the transaction.
- An applicant is very interested in “free-look” periods that allow for a return of premiums after a policy cancellation but expresses little concern about other aspects of the product.
- Personal identification cards have suspicious pictures or suspicious dates on them.
- Policy ownership is transferred without a reasonable explanation.
- A consumer is engaging in an irregularly high number of insurance transactions.

Despite all of these potential warning signs of money laundering, it is important to remember that an individual red flag has a chance of being nothing more than a false alarm. When evaluating red flags in accordance with a company’s anti-money laundering program, professionals shouldn’t be afraid to use common sense or to seek advice from management.

Also, companies and individuals may find that anti-money laundering techniques sometimes clash with a consumer’s expectation of privacy. This is especially true if an insurance professional decides to question an applicant whose interest in a particular product lacks a logical explanation. Companies may want to evaluate their anti-money laundering programs carefully so that their crime-prevention efforts don’t violate professional ethics or a person’s legal rights.

Checking Government Lists

The previous section mentioned the Financial Action Task Force and its list of countries that have been known to take money laundering less seriously than others. This list can be helpful in running an effective anti-money laundering program in compliance with BSA rules.

Note, however, that checking certain lists is not only an important task for companies that need an anti-money laundering programs. According to legal experts cited in multiple trade publications (such as Business Insurance and National Underwriter), even an insurance company that doesn't need to comply with the Bank Secrecy Act might still need to crosscheck its customers against lists of suspected or designated terrorists from the Office of Foreign Asset Control. According to those sources, this requirement might even apply to property and casualty insurers, health insurers and other insurance-related entities that aren't considered to be a target for money laundering.

Role of Compliance Officers

An insurance company's anti-money laundering program must be overseen by a compliance officer. The officer can be one person or a group of people but must be someone with the authority to implement the program across all departments and who has strong knowledge of how the insurance company operates.

The amount of hours spent on anti-money laundering activities will depend on the intricacy of the program, the size of the organization and the company's level of risk. But regardless of the size of the job, the compliance officer is expected to have the following responsibilities:

- Implementing a program that reflects the insurer's level of risk.
- Making updates to the program as necessary.
- Remaining up-to-date on FinCEN requirements.
- Coordinating anti-money laundering training programs for employees and agents.
- Answering questions from employees, agents and others about the program.

Program Audits

An insurer's anti-money laundering program must continue to reflect the company's level of risk and be in compliance with the latest FinCEN requirements. In order to ensure that the program remains effective and up to date, the program must be audited by an unbiased person. The insurer can hire a third party to conduct the audit or have the audit performed by its employees. However, anyone who is serving as the program's compliance officer cannot also serve as its auditor.

Audits should be done whenever a company's level of risk related to money laundering is likely to change. For example, an audit might be in order if the company starts offering new kinds of products or starts targeting a new type of customer. There is no specific timeframe or deadline (such as every year or every six months) for conducting mandatory audits.

When an auditor notes potential problems with an insurer's anti-money laundering program, the auditor's findings and recommendations should be put in writing. Copies of the written audit should be provided to the compliance officer and senior management.

Compliance for Variable Insurance Products

Broker-dealers and other organizations that offer variable life insurance or variable annuities are likely to have additional anti-money laundering requirements because they sell securities. In addition to federal laws and the various BSA rules, regulations from FINRA (the main non-governmental regulatory body for the securities industry) should be reviewed by these entities. If a company sells insurance and securities, it may need different anti-money laundering procedures depending on the type of product being sold.

Mandatory Producer/Employee Training

Insurance companies with an anti-money laundering program must ensure that the people working for them are properly trained to detect possible money laundering and to follow proper procedures. The specifics and scope of the training should reflect a person's role within the organization and his or her potential exposure to money laundering schemes. For some people at the insurance company, the training might be relatively intensive. For others, the training might be very basic.

Mandatory training can be handled internally by the insurance company or outsourced to a competent third party. Examples of a possibly competent third party include another insurance company, a bank, a broker-

dealer or any other company that is required to have its own anti-money laundering program. At the time this material was being written, there was no required format for the training. For example, training might be done in person at a company meeting, in person in a formal classroom setting, in a hard-copy written format or over the internet. Training programs are not approved by FinCEN and do not need to be approved for continuing education credit by a state's insurance department. However, an insurance company's compliance officer must review the content of the training and believe it is satisfactory. A more thorough evaluation might be required if the training provider doesn't have its own anti-money laundering program.

Insurance agents and brokers don't need their own anti-money laundering programs and don't need to complete anti-money laundering training in order to maintain their insurance license. The responsibilities of establishing a program and ensuring adequate training of individuals have been reserved for insurance carriers (not individual licensees) because carriers are more likely to have the resources to establish a program and are likely to already have similar training programs in regard to fraud prevention.

Still, it is very likely that an insurer's anti-money laundering program will involve participation from agents and brokers and have internal training requirements for those licensed salespersons. Agents and brokers are in the front lines in the battle against fraud and money laundering and are often the best sources of information about applicants and policyholders. Since they tend to know their customers, they are likely to have an important perspective regarding red flags and whether a particular person might be engaging in illegal behavior.

Agents and brokers must comply with an insurance carrier's anti-laundering program. In the event that an agent or broker doesn't follow proper procedures, the company's designated compliance officer is expected to take corrective action. In serious cases, the insurer might decide to sever its relationship with the agent or broker.

Suspicious Activity Reports

A key component of an anti-money laundering program is the proper filing of "Suspicious Activity Reports" (SARs) with FinCEN. These special reports involve the use of specific government forms and must be filed with FinCEN when an insurer notices suspicious activity involving at least $5,000 in assets. For example, a transaction involving that amount (in cash or otherwise) would need to be filed under any of the following circumstances:

- The funds used in the transaction seem to be derived from illegal activity.
- The transaction seems designed to hide illegal funds.
- The transaction seems designed to facilitate illegal activity.
- The transaction is unusual and is done without any reasonable explanation.
- The transaction involves less than $5,000 but seems designed to avoid the filing of a report.

In spite of these general requirements, there are many cases in which a suspicious transaction might not require the filing of a report. For example, SARs do not need to be filed in connection with transactions that do not involve covered products. (Again, covered products are generally limited to cash-value life insurance and annuities.) Similarly, a report does not necessarily need to be filed when possibly illegal activity doesn't involve money laundering or terrorism. For example, according to federal guidance, a report would not necessarily need to be filed in the case of an applicant who has lied about medical issues in order to obtain life insurance.

Individual insurance producers are not expected to file a report on their own without involvement from their insurance carrier. However, they are important to the reporting process because they are likely to provide important information that a carrier will need to complete a report. Agents and brokers who do not follow a carrier's anti-money laundering program will prevent insurers from satisfying the company's reporting requirement.

SAR Deadlines

SARs must be filed within 30 days after an insurer notices suspicious activity and can identify who is doing it. If the person behind the suspicious activity is unknown, the insurer can take an additional 30 days to

investigate. However, in an emergency situation, such as a clear link to terrorism, the insurer is expected to contact law enforcement immediately. The SAR deadlines don't release the insurer from having to respond right away in an emergency.

Completing SARs

SARs fail to serve their purpose when they are filed incorrectly. With this in mind, FinCEN has stressed the importance of providing sufficient details about a suspicious transaction in a report's main "narrative" section. This section should answer five basic questions concerning the suspicious transaction: who, what, where, when and why?

Answers to the first four of those questions should provide the facts of the suspicious transaction. Once those facts have been provided, the insurance company should explain why the facts of the transaction are considered suspicious.

All relevant information should be provided on FinCEN's SAR form. At the time this course material was being written, the government was not accepting attachments to these forms.

Individual documentation about the suspicious transaction should be maintained by the insurer for at least five years. If FinCEN requires additional information, it will contact the insurer via the contact items provided on the SAR form.

SAR Confidentiality

Financial institutions are obligated to keep the existence of SARs confidential. An insurer is forbidden from informing customers that a report has been filed about them. If information related to a report is subpoenaed, the insurer should contact FinCEN for instructions.

In general, the only parties who can be told about SARs are law enforcement entities, other financial institutions (in limited circumstances) and the insurer's management team.

Reporting Large Transactions

Insurance companies are required to fill out a special report when they receive $10,000 or more in cash in one transaction or in related transactions. This requirement preceded the other BSA rules mentioned in these materials and must be made separately from a Suspicious Activity Report. This currency report must be made regardless of whether the transaction seems suspicious.

Conclusion

Terrorism prevention should be a priority for practically everyone in the United States, and insurance professionals are no exception By being observant and following some basic federal guidelines, insurance licensees can play a small yet very important role in keeping our country safe.

CHAPTER 2: INSURANCE DISCRIMINATION - THEN AND NOW

Introduction

For most people in our increasingly diverse society, the word "discrimination" tends to bring uncomfortably negative images to mind. Some of those images—protesters clashing with local authorities during the Civil Rights movement, or signs for racially segregated public accommodations in the Jim-Crow-era South—are familiar to us from the historical record. Others—such as that of the veteran female receptionist who is curiously passed over for promotions by male bosses—aren't as graphic and tend to come to our attention through the anecdotes of friends and family or from our own personal experiences. In part to avoid seeing those unpleasant pictures, we might try to convince ourselves that discrimination is either a thing of the past or at least something that would never be tolerated in our own business.

However, discrimination can be a fascinatingly complicated subject for insurance professionals. This is particularly possible if we detach the social connotations from the word and focus purely on its basic definition. Discrimination, at its most elementary level, occurs whenever two or more people are evaluated in some way (fairly or otherwise) and then treated in different ways on the basis of that evaluation. If we

keep this emotionally neutral definition in mind, we may notice that discrimination is not only common but central to the operation of our industry.

To demonstrate this point, think of the line of insurance in which you have the greatest amount of expertise. Is this insurance made available to some applicants but not others? Is this insurance offered at the same price to everyone? Even if the insurance is offered as part of a guaranteed-issue group plan in which all participants contribute the same amount of premiums, are there differences in pricing from group to group? Unless the insurance is offered to all interested applicants at exactly the same price, some form of discrimination is technically taking place.

Often, arguments that are seemingly about whether discrimination exists are really about whether a particular kind of discrimination is ethical and fair. At least in regard to insurance practices, state regulators have already participated in those arguments and arrived at some clear conclusions for us. For example, insurance commissioners across the United States have generally determined that discriminating against consumers on the direct basis of race, religion or national origin is inappropriate and have made this discrimination illegal. (This is a contrast with many other countries—even developed areas like Western Europe—where insurers sometimes apply different rates to foreigners and non-foreigners.)

While some of the prohibitions against insurance discrimination might seem obvious, perceptions of fairness continue to evolve. Traditionally, insurers and their customers have agreed that discrimination is justified when it is based entirely on a person's risk potential and is backed up by sound actuarial data. But as the underwriting process has become more complex, even insurers with data on their side have had a harder time making their case.

Consider, for example, the U.S. auto insurance market, where credit history—and not driving history—might have the biggest impact on a driver's auto insurance premiums. Even as the numbers consistently link the likelihood of auto insurance claims to a person's bill-paying activities, many motorists believe, for various reasons, that credit-based insurance decisions are unfairly discriminatory.

At times, the arguments concerning discrimination are about whether a person's risk profile should even matter at all. The passage of the Affordable Care Act provoked heated debate regarding the best way to cover the uninsured against illness or injury. But while verbal battles were waged about mandates and the law's rollout, more Americans seemed to come away with the belief that all people—even the very sick—should have access to affordable, high-quality health insurance.

Although this course material will lay out the many arguments for and against certain insurance practices, it shouldn't be interpreted as a political document or as a piece of advocacy. Where matters of anti-discrimination law are addressed, the intent is to promote compliance with federal and state requirements. In cases where the labeling of a particular insurance practice as "fair" or "unfair" is still a matter of major debate, readers will be given enough context to understand both sides of the issue. If you have a firm understanding of what each side believes, you might be able to play a role—small as it may be—in building a consensus.

Racial Issues in Insurance

Race-related issues in insurance date all the way back to the pre-Civil War era, when insurers viewed slaves as property and insured them as such for their white owners. After that war but prior to the Civil Rights movement, insurance companies commonly relied on loss-related data to charge different amounts depending on whether a consumer was white or black.

Race-based pricing was especially common in life insurance and was practiced with regulators' blessings due to the significant disparities in life expectancies between minorities and non-minorities. As reported by the Wall Street Journal, for example, white Americans were on pace to live roughly seven years longer than black Americans in 1955. Statistics like that were at least partially responsible for African Americans being charged sometimes as much as one-third more than other customers.

The significant differences in price didn't always mean that life insurers weren't interested in marketing themselves to communities of color. However, when those communities were targeted, companies and their agents tended to emphasize non-traditional products. Instead of stressing usual forms of life insurance with

significant death benefits, insurance salespersons went door to door and peddled small burial policies that covered final expenses in exchange for weekly or monthly payments of a few dollars. Even in these instances of targeted sales, race-based mortality tables were used to price the products.

In some cases, the risk-related data that was used decades ago by insurers hasn't changed much. Racial disparities still exist in regard to the quality of health care received by minorities vs. non-minorities, and according to the Centers for Disease Control, white Americans continued to have longer life expectancies than African Americans (by roughly four years according to 2018 figures) . But regulators and the general public have been reinterpreting those numbers ever since the days of the Civil Rights movement. To many observers, those numbers should be ignored because they are more likely the result of economic factors (such as higher poverty rates among minorities) rather than being directly related to race. Even among those who don't fully accept this poverty-linked hypothesis, the use of race-related data to offer or price insurance seems contrary to their morals. For these reasons and more, direct forms of racial discrimination in insurance have been made illegal by state or federal laws in practically all cases.

For sellers of burial insurance, the changes in laws and in societal views put an end to race-based pricing in the issuance of new policies. But many policyholders who had purchased coverage prior to the ban continued to pay the same monthly or weekly installments for decades. According to a report by the state of Florida, 29 U.S. life insurers had not corrected race-based pricing models for pre-existing policyholders by the year 2000. Several class-action suits have been settled in the decades since the report.

Despite the ban on direct racial discrimination, some sociologists and civil rights activists are convinced that racial minorities are still not always treated fairly by insurers. As evidence, they often cite the results of "matched-pair" studies. In a matched-pair study, individuals inquire about insurance (usually from property and casualty agents) and take note of their treatment. Individuals who are part of the study will have the same risk profile but will be members of different racial groups.

Multiple matched-pair studies have at least hinted at the presence of racial discrimination at some property and casualty insurance businesses. When leaving messages at these businesses, white callers have sometimes been more likely to have their calls returned. Similarly, individuals posing as insurance applicants have sometimes noted differences in their ability to obtain an insurance quote depending on their race. On the other hand, critics of those studies have sometimes noted the usually small sample sizes of the data.

Redlining

Several decades ago, it wasn't uncommon for maps at real estate and lending offices to be marked with red lines, indicating where business was not to be done. Very often, the marked areas were low-income communities where large amounts of racial minorities lived. By marking those areas and refusing to do business in them, companies were ultimately accused of sidestepping the requirements of various civil rights laws that prohibited discrimination on the basis of race. This practice became known as "redlining."

Alleged redlining has often been a problem in communities where rioting has occurred. After race-related riots in the late 1960s prompted an exodus by insurers out of some urban areas, the federal government made reinsurance available to carriers in any state that instituted plans for covering property in seemingly high-risk areas. Though this kind of financial protection for insurance companies is now offered primarily by reinsurers in the private market, the original mechanism for serving high-risk applicants —known as a FAIR plan—still can be found in practically all states.

Decades later, following riots that resulted after alleged police brutality against African-American man Rodney King, businesses in the South Central portion of Los Angeles struggled to reopen due, at least in part, to the unavailability of affordable property and casualty insurance. Accusations of redlining returned and prompted government and industry to reexamine the issue.

Defining Redlining

Discussions about the prevalence of redlining can be stressful because there are many opinions regarding what the term actually means. The debate about terminology relates both to the intent of insurers' actions in certain communities and to the impact—regardless of intent—that those actions have on residents.

To some, redlining only occurs when an insurer flatly refuses to insure properties (or provide other kinds of coverage) in a particular geographic area. To others, it can also include cases where insurance is technically available in all areas but is viewed as prohibitively expensive in certain neighborhoods.

In either of those cases, some people have an even stricter definition and argue that redlining only occurs when the reason why an insurer won't offer affordable coverage in a neighborhood is based on the types of people living there. Conversely, others argue that redlining can occur even if an insurer claims to only be basing its business decisions on environmental risk factors and not specifically on the race, ethnicity or other personal characteristic of the typical resident.

Location and Risk

From many insurers' perspectives, several risk-related reasons exist for pricing and offering property and casualty insurance differently in certain neighborhoods. When questioned about business practices that treat urban areas (particularly the dense inner-city) less favorably than other communities, insurers tend to cite the following rationales:

- Some urban areas tend to have higher crime rates, including for theft and arson.
- Some urban areas have a disproportionate amount of vacant buildings, which could lead to vandalism or other kinds of damage.
- Some urban areas have an especially high amount of older buildings, which might be in disrepair or have lower market values.
- Urban areas have many properties that are close to one another, which can multiply the impact of a fire, tornado or catastrophic event.
- For auto insurers, urban areas have more traffic, which could result in more accidents.

It should be noted, however, that rural areas present their own set of risks. For example, rural homes are likely to be far away from emergency services, and local roads might make it more difficult for police or fire departments to reach the site of an accident.

Redlining and State Regulation

In general, states have frowned on insurers that have attempted to completely avoid doing business in certain communities. This has been the case even when racial or ethnic factors have been absent from the conversation. For an example, consider property insurers that have been spooked by natural disasters in coastal areas, such as parts of Florida. Many of those insurers have learned that if they don't want to provide coverage at all for properties in certain high-risk neighborhoods, they must take the same position toward the rest of the state and will be required to exit the entire market if they don't want to serve a particular area.

Less uniformity exists nationwide regarding the pricing (as opposed to availability) of insurance based on geographic location. Whereas most states allow for some form of territorial rating that makes insurance cost different amounts based on an applicant's location (usually by ZIP code), some put significant limits on those practices. For example, voters in California approved a measure that requires auto insurance rates to be based primarily on a person's driving history and minimizes the impact of a vehicle's usual location.

Where territorial rating practices are permitted, civil rights organizations sometimes raise concerns about how the differences in pricing are impacting minority communities. Depending on the circumstances, they might pose the following questions to insurers, courts or regulators:

- Does territorial rating give insurance companies an opportunity to discriminate intentionally against minorities?
- If territorial rating ends up having a disproportionate but unintentional impact on minorities, should it be allowed?
- Does territorial rating allow insurers to make overly broad judgments about applicants rather than forcing them to look at each applicant's individual risk profile?

Redlining Disclosure Requirements

Groups and individuals who are especially concerned about redlining are typically in favor of laws that would require insurers to report various pieces of demographic data to insurance regulators. The data might include information about an insurer's market share in various communities as well as the race or ethnicity of each applicant and how the applicant's request for insurance was handled.

This kind of requirement already exists at the federal level for mortgage professionals. Under the Home Mortgage Disclosure Act (HMDA), lenders must send specific kinds of information (including the race and ethnicity of loan applicants and whether a loan was approved or denied) to federal agencies, but the law does not extend to the insurance community. Similar insurance-related laws have been proposed at the federal level for decades but have failed to gain much traction.

States have taken different approaches to the issue. Some require race and ZIP-code level reporting to their insurance department. Some require that this data be gathered but only sent to regulators upon request. In other parts of the country, no such reporting is required at all.

Rather than believing that HMDA-like reporting would help prove a lack of discrimination in their business practices, insurance companies have generally opposed these types of requirements. Commonly stated reasons for their opposition appear next:

- Insurers that are shown to be less prominent in minority neighborhoods might be sued even if they had no intention of discriminating against minority groups.
- Applicants who are asked about their race or ethnicity for the purpose of data collection might object and worry about how the information will be used.
- Requiring insurance agents to obtain information about race or ethnicity increases the chances of unethical agents being influenced by the information.
- If information about an insurer's market share in certain neighborhoods is reported and becomes public, competitors might benefit unfairly from the disclosure.
- Insurance regulation has generally been left to the individual states. Federally mandated reporting would conflict with this tradition.

Insurers that don't want greater regulation but are still concerned about risks in certain neighborhoods might want to consider proactive ways in which they can protect their bottom line while still serving all communities. For example, some commentators have suggested education campaigns that are meant to make property owners more aware of how they can reduce their insurance premiums with the help of burglar alarms, smoke detectors and other loss-prevention tools.

Similarly, rather than evaluating applicants on a broad ZIP-code level or by the age of a dwelling, underwriting departments might consider ways in which properties can be evaluated on more of a case-by-case basis. For instance, property insurers might consider being open to the idea of offering cheaper insurance to the owners of an otherwise old building that has been either retrofitted to withstand disasters or rewired to reduce fires.

Disabilities and Pre-Existing Conditions

The high cost of health care in the United States helps explain why people's health history has been such an important factor in offering and pricing many kinds of insurance. At the same time, the universality of health-related concerns has made medical underwriting a topic of heated debate. Since we will all inevitably become sick or suffer some kind of physical injury in our life, it's not difficult for us to sympathize with fellow human beings who experience negative insurance-related consequences on account of a pre-existing medical condition. As a society, we seem to be moving much closer to believing that health-related discrimination should be avoided in most cases unless a person's physical problems are tied to smoking and other unwise lifestyle choices.

A consumer's health can have an impact on the cost or availability of many insurance products. It is a major factor in life insurance underwriting and disability insurance due to carriers' concerns about mortality and morbidity, respectively. It can even have an indirect impact on some kinds of property and casualty

coverage, too. Businesses with a history of injured workers will pay more for workers compensation insurance, and, according to a survey discussed in the trade publication American Agent and Broker, disabled drivers often even pay more for personal auto coverage.

But of course, no other kind of insurance is affected by health more than health insurance. State and federal laws over the past few decades have tightened restrictions on various kinds of medical underwriting and have even eliminated the practice in some markets. Many of those legislatively imposed restrictions will be covered in the next several sections. However, as you read about laws like the Affordable Care Act and others, you might find it interesting to note the ways in which the attempts to eliminate one form of discrimination—in these cases, health discrimination—have perhaps heightened the existence of other forms of alleged discrimination (such as discrimination based on age). Rightly or wrongly, anti-discrimination requirements in insurance are not a full guarantee that all consumers will receive the same insurance at the same price.

The Health Insurance Portability and Accountability Act

Not unlike the lawmakers who debated major health reforms in 2009 and 2010, elected officials in the early-to-mid-1990s fought fierce battles over what role the government ought to play in the U.S. health care system. Although opponents of greater federal involvement successfully beat back the Clinton administration's attempt at achieving universal insurance coverage, people on both sides of the argument agreed that a problem known as "job lock" needed to be addressed.

At a time when technological innovations were sparking many people's desire to open new businesses, some workers still clung nervously to their same old jobs. As much as they may have wanted to pursue opportunities at different companies, workers with pre-existing health problems had no guarantee that they would be eligible for coverage through a new employer's insurance plan. Likewise, even if a healthy employee could count on getting self-only coverage through a new job, he or she couldn't bet that the person's cancer-surviving spouse or diabetic child would be eligible too. Rather than risk losing essential health benefits for themselves and their families, these workers would often play it safe and stay in unfulfilling careers.

The Health Insurance Portability and Accountability Act (HIPAA) attacked the problem of job lock by making it illegal for a group health plan to discriminate against someone (including dependents) on the basis of health. As simple as that prohibition may seem, we won't be able to fully grasp its importance unless we know what is meant by words like "discrimination" and "health" within the context of HIPAA.

At least as far as HIPAA is concerned, a group health plan would be discriminating against someone in all of the following cases:

- The person is denied membership into the group plan.
- The person is required to pay higher premiums than other group members.
- The person is provided fewer insurance benefits than other group members.
- The person is required to make higher co-payments than other group members.
- The person is required to pay higher deductibles than other group members.
- The person is required to wait longer for coverage to begin than other group members.

Though there are some factors that could cause someone to be discriminated against in a group plan, health can't be one of them. Therefore, an individual can't be treated differently because of:

- A physical or mental condition he or she currently has.
- A physical or mental condition he or she previously had.
- A person's history of making health insurance claims.
- Genetic information that suggests a person is susceptible to medical problems.

- Behavioral, lifestyle or environmental factors that suggest a person might file health insurance claims (such as playing extreme sports, being in a physically abusive relationship or having made a suicide attempt).

One thing you'll realize quickly about HIPAA, though, is that there are plenty of exceptions to its rules and plenty of particulars to keep in mind.

Does Everyone Get Covered?

Although HIPAA prohibits discrimination on the basis of health, it doesn't force employers to offer coverage to all of their employees. It only prevents them from denying participation in a group plan for medical reasons.

So, for example, the law doesn't force an employer to have a health plan, and it doesn't stop the health plan from discriminating against people for non-health reasons. A plan that covers full-time employees but excludes part-time workers isn't violating HIPAA. (A requirement to have a group health plan at companies with 50 or more full-time employees was instituted several years later under the Affordable Care Act.)

HIPAA Exemptions

Group plans that aren't health plans are generally exempt from HIPAA's nondiscrimination requirements. This is true even when benefits are triggered by a person's medical problems. For example, the rules generally don't apply to:

- Workers compensation.
- Group disability insurance.
- Group life insurance.
- Group accidental death and dismemberment insurance.
- Group auto insurance.

Dental, vision and long-term care insurance offered through a group aren't subject to HIPAA's nondiscrimination rules if either of the following is true:

- They're offered under a different contract, certificate or policy than other health insurance.
- They're provided to employees for an additional cost, and employees can choose not to take them.

Can You Reward Healthy People?

Many group health plans reward people who have healthy lifestyles. For example, it's not uncommon for employees to pay less for their health insurance if they maintain a good weight or don't smoke.

There are obvious benefits to having a healthy workforce, but employers and group plans need to understand that a person's weight and smoking habits are considered health factors. Therefore, giving preferential treatment to non-smokers or thinner people can amount to a HIPAA violation if special rules aren't followed.

Plans that reward healthier people are allowed if they give unhealthy people an alternative way of qualifying for the same reward. For instance, a plan rewarding non-smokers might also opt to reward smokers who enroll in a smoking cessation program. A plan rewarding physically fit employees might also opt to reward overweight employees who agree to follow an exercise regimen.

Let's go over more of the rules for these kinds of plans. Be aware, however, that, like all the law-related information in this course, the information is intended for general purposes. Due to the complexity of legal issues, you should seek out an expert if you have specific questions about how the law impacts you.

Rules for Wellness Programs

Programs that promote health to group members are known as "wellness plans" or "wellness programs." Companies have found that the best way to increase participation in a wellness program is to offer direct financial incentives to their employees. These incentives might include cheaper health insurance, a waiver of certain deductibles or the chance to receive gifts.

If a company is planning on offering incentives to employees as part of a wellness plan, the incentives can't be given on a discriminatory basis. Rewarding employees for simply participating in a wellness program isn't discriminatory. But tying those incentives to an employee's personal health can be against the law.

To be compliant with HIPAA, a wellness plan that rewards anyone for their health must adhere to several rules. Let's go over them one by one.

Design of the Plan

The wellness plan must be designed to promote health in a reasonable way. It is illegal to design something with the intent of discriminating against someone and then try to pass it off as a wellness plan.

Chances to Qualify

Employees must be given the chance to qualify for the wellness plan at least once a year.

Size of Rewards

No matter the kind of reward a wellness plan offers, the value of the reward can't be greater than 30 percent of the cost of covering the individual. The cost of coverage includes the portion paid by the employee and the portion paid by the employer. It can also include the cost of insuring the employee's dependents if they are eligible to participate in the wellness plan.

Reasonable Alternatives

If a wellness plan is going to reward people for being in good health, there needs to be a reasonable alternative way for unhealthy people to qualify for the same reward. The alternative is reserved for cases in which adhering to the plan's regular standards would be unreasonable for a particular employee or would put the employee's health at risk.

For a few examples, let's think back to plans that reward people for not being overweight or not smoking. Since it would not be reasonable or medically advisable for a significantly overweight employee to slim down dramatically over a very brief period of time, the employee might have the alternative option of enrolling in an exercise program. Since it would be unreasonable to expect a lifelong smoker to suddenly quit the habit all at once, an employee might be given the alternative option of enrolling in a smoking cessation program.

Reasonable alternatives for wellness plans can't force employees to achieve a particular health-related outcome. For the employee enrolled in the exercise program for example,, this means the plan can't require that the person slim down to a certain weight or body-mass index. For the employee in the smoking cessation program, it might mean that the person still can't be forced to quit. In both examples, simply participating in the program would likely need to be enough for the employee to be rewarded.

Though plans need an alternative for their wellness programs, they have some leeway in deciding what the alternative should be. As long as it is reasonable for all employees, a single alternative can be used for everyone in the group. On the other hand, a plan has the option of tailoring the alternative to an employee's individual needs. If, for instance, a disability prevents an employee from enrolling in an exercise program, the plan can work with the person to come up with another way of qualifying for the reward.

If a reasonable alternative can't be found for a particular employee, the plan might simply waive eligibility requirements for that person. In any case, the plan can require a doctor's note in order for someone to be eligible for a reasonable alternative.

Notice of Alternatives

All materials that describe a wellness plan to employees must mention the existence of a reasonable alternative. They do not need to mention what the alternative is. That can be worked out between the plan and the employee.

For compliance purposes, the U.S. Department of Labor has suggested using the following language in a wellness plan's materials:

- *If it is unreasonably difficult due to a medical condition for you to achieve the standards for the reward under this program, call us at (insert plan's telephone number) and we will work with you to develop another way to qualify for the reward.*

The Affordable Care Act

The Affordable Care Act (sometimes known as "Obamacare") is a massive, complex law that prompted several major changes to our country's health care system. However, many of the changes were intended to serve the same purpose: making it simpler for unhealthy people to find and keep affordable health insurance coverage.

Prior to the law's implementation in 2014, health insurance could be tough to find if you had already been treated for a major medical problem. If you were applying for coverage and were treated for a serious issue within the last few years, a plan in the individual market (as opposed to the group market) might have refused to cover you at all. If you had been sick within the past six months and applied for group coverage, the group plan could have subjected you to a waiting period before paying for any treatment related to that ailment. For some group members, the waiting period for treatment of pre-existing health problems lasted up to 18 months.

Under the Affordable Care Act, applicants for health insurance can no longer be denied insurance because of a pre-existing health condition. Once they're accepted by a plan, there can't be any waiting period for benefits because of a pre-existing condition. Unhealthy individuals will be eligible for practically any kind of health insurance on the market as long as they purchase it during an annual open enrollment period.

Restrictions on Premium Rates

Shoppers in the health insurance market will discover that the Affordable Care Act's anti-discrimination provisions don't just pertain to access to insurance. They relate to pricing as well.

As a result of the law, insurers in the individual and small-group markets are generally prohibited from charging people more because of personal health. Gender-based pricing is now illegal in these markets, too. In fact, when two people (or two small groups) purchase exactly the same kind of health insurance, only the following factors can be used to charge them different rates:

- Age (with the cost for one age group equaling no more than three times the cost for any other age group).
- Tobacco use (with the cost for smokers equaling no more than 1.5 times the cost for nonsmokers).
- Geographic rating area (as determined by each state).
- Whether the insurance is for an individual or a family.

In essence, the rating reforms mean people in the individual market will be charged as if they were part of a large group. Although the cumulative health status of their geographic rating area might impact the cost of insurance, their own health status won't have much of an effect on what they pay.

People in the small-group market were already part of a pool for the purpose of pricing, but the new rules make the size of that pool much bigger. For better or worse, the risk of insuring unhealthy people will be spread out and shared among a broader population.

The rules about rating generally don't apply to "grandfathered plans." At a basic level, grandfathered plans are individual and group health plans that already existed on March 23, 2010 (when the law was passed), and haven't undergone significant changes since then.

As you can see, the requirements of the Affordable Care Act eliminate some forms of discrimination but still don't treat all applicants in a completely equal fashion. For example, the law allows insurers (and group plans) to charge people more based on their age, and although health factors are generally no longer a part of underwriting in the individual market, shoppers might still pay more if they smoke.

In spite of the summaries provided here, be aware that the Affordable Care Act is a complicated law that is still in the process of being implemented. Furthermore, at the time this course was being written, the law was still being subjected to various legal challenges in the court system, which could result in major changes

to what's detailed here. For those reasons and more, if you are in charge of compliance at your business, you should consider contacting an expert or researching this law more closely through the U.S. Department of Health and Human Services.

Mental Health Parity

As mental health has become less of a stigmatized topic, the insurance-related rights for individuals with mental health problems have grown. In 1996, Congress passed the Mental Health Parity Act, which required lifetime and annual dollar limits for mental health care to be equal to the dollar limits for physical health care. The law didn't require coverage for mental health care, and insurers who were providing such coverage could still have different limits for mental health if those limits weren't based on annual or lifetime dollar limits. For example, a plan could still have different copayments or coinsurance fees for mental health and could put different limits on the number of covered visits. The law applies to group plans with more than 50 members.

The Mental Health Parity and Addiction Equity Act of 2008 expanded upon the requirements of the earlier law. Under the act from 2008, plans covering mental health care must have substantially the same limits for mental health care and physical health care in regard to most aspects of coverage, including deductibles, coinsurance fees, copayments and number of visits. As with the earlier law, it doesn't force plans to cover mental health care in the first place, It applies to group plans for more than 50 people and, as a result of the Affordable Care Act, also is applicable to policies sold in the individual market.

Many states require coverage of mental health care in some plans. In just one of many possible examples, Illinois requires group plans for more than 50 employees to cover "serious mental illnesses." Insurers offering plans to smaller groups in the state must offer mental health coverage to the employer, but the employer can decline it. At the federal level, the Affordable Care Act required most non-grandfathered health insurance plans in the group and individual market to cover mental health services and prohibited lifetime and annual caps on those benefits. However, the specifics of what kinds of mental health care needed to be covered were left up to the individual states.

Genetic Information

Thanks to the wonders of modern science, medical tests have the potential to dissect our DNA and determine whether our genetic material makes us especially susceptible to certain diseases. Although genetic tests generally won't guarantee that we will develop a given medical condition, their results can help interested people manage certain risks. If a man and a woman both test positive for a particular genetic condition, they might take the results into consideration before having children together. If a young adult tests positive for a gene linked to cancer or Alzheimer's disease, the person might allow this information to influence his or her lifestyle choices and financial plans.

In spite of the advances in genetic detection, not all patients believe that genetic tests make sense for them. To some, the testing can amount to knowing too much about one's future and can lead to serious distress if test results suggest the likelihood of a debilitating condition. To others, a genetic test lacks much value unless it can conclusively prove that a medical condition will, in fact, manifest itself. In other words, although they might not have a problem with testing to see if they conclusively have a particular illness, they see little point in a test that only proves that they are at a higher risk for the disease.

Even among people who believe genetic testing has its benefits, there continues to be widespread trepidation regarding how genetic information might be used by third parties. If the results of a test become known to an employer, might a worker suffer workplace discrimination so that the business can save money on its various insurance plans? If results of a test become known to an insurer, might the information cause the person to be disqualified or charged more for life, disability, health or long-term care insurance? Might an insurer require a genetic test in some cases even if the patient doesn't want to know the results? And if a test reveals that a person's genetic code makes him or her a higher risk for contracting a specific disease, will an insurer treat it as a pre-existing condition and refuse to cover any eventual treatment for that disease?

Based on those concerns, it's likely that many patients who would otherwise be interested in genetic testing have declined to learn more about their hereditary medical risks. Some doctors have counseled against

having the tests because of discrimination and privacy issues, and many patients who get these tests will pay in cash so that their insurer is less likely to know about them.

Although cases of genetic discrimination by employers and insurers are relatively rare, the public's fears surrounding this form of discrimination are real. According to a poll referenced in 2009 by the New York Times, 63 percent of people would refuse to take a genetic test if either an employer or an insurer were likely to learn the results. Such concern, according to the scientific community, makes it harder for researchers to conduct genetic studies that could lead to life-changing discoveries. The National Institutes of Health has said that 30 percent of people who are approached to be part of genetic research projects decline because they are worried about possible discrimination.

Despite the public's many concerns, some insurance companies don't see a problem in using genetic information to offer or price their products. Insurance, after all, has historically been offered in connection with an applicant's risk profile, and a person's genetics are, indeed, an indicator (if not an absolute predictor) of medical risks. To some inside the industry, genetic information seems like the perfect tool for evaluating someone for various forms of accident and health insurance.

Insurers also note the possibility for unfairness if applicants are allowed to receive genetic testing results without having to disclose the information on an insurance application. If, for example, a consumer knows that he or she is at greater risk of contracting Alzheimer's disease, it seems more likely that the person will be interested in long-term care insurance. But if that applicant (and people in similar situations) isn't required to disclose their increased risk, there is a chance that the market for long-term care insurance will become overcrowded by people with this increased risk. This problem, known as "adverse selection," could destabilize the market and result in either higher prices or even insolvency among insurance carriers.

The Genetic Information Non-Discrimination Act

By 2008, nearly every state had passed laws that protected the public's genetic information. However, requirements weren't consistent across the country, and self-insured businesses that operated their own health plans under the Employee Retirement Income Security Act were generally exempt from state-level anti-discrimination rules.

Greater uniformity was achieved through nearly unanimous Congressional support of the Genetic Information Non-Discrimination Act (commonly known as "GINA"). This federal law went into effect in 2009 and prohibits discrimination by health plans and health insurers on the basis of genetic information (including the medical history of family members). In practical terms, this means a health insurance company or health plan cannot take any of the following actions:

- Deny eligibility for insurance because of someone's genetic information.
- Charge people more because of their genetic information.
- Use genetic information to categorize an ailment as a pre-existing condition.
- Require individuals to take genetic tests as part of the enrollment or application process.

Although some genetic protections already existed under HIPAA, those protections generally didn't help people outside of group health plans, and they didn't stop a group from being penalized as a whole because of the cumulative genetics of its members.

In spite of these protections, GINA doesn't stop insurers or group plans from taking any of the following actions:

- Discriminating against people on the basis of a medical condition that has actually materialized and been diagnosed. (For example, a person whose genes make him or her a high risk for cancer but hasn't been diagnosed with cancer would be protected by GINA. However, someone who already has a genetic form of cancer would need to rely on protections under other laws, such as HIPAA and/or the Affordable Care Act.)
- Refusing to cover the cost of genetic tests.

- Limiting certain kinds of covered care to people who have certain kinds of genetics. (For example, some kinds of preventive care might only be covered by insurance if a person's genetics make him or her a high risk for a particular condition.)
- Discriminating on the basis of genetic information in the life insurance, disability insurance or long-term care insurance markets. (However, be aware that this form of discrimination might be prohibited by state laws.)

Gender Discrimination

When an insurance company prices its products without any gender-based differences, it is engaging in "unisex rating." The arguments in support of unisex rating are somewhat similar to those against race-based rating practices. Like a person's race, gender is not something that is chosen by the individual at birth. Due to this lack of choice, many people believe insurance companies should not price their policies in different ways across gender lines. They make this case even as insurers point toward risk-related data that seem to separate the sexes.

Unisex rating, while not practiced by all U.S. insurers, is becoming more common among carriers in other parts of the world. When males in Europe complained that charging them more for life insurance was discriminatory, the European Court of Justice—the highest court in the European Union—agreed with them. The ruling struck down discriminatory practices in more than 25 countries. The court's decision, though, had no impact on companies in the United States.

Americans are generally protected from gender-based insurance discrimination when they obtain coverage through an employer's group plan. Laws like the Civil Rights Act of 1964, the Equal Pay Act and HIPAA collectively prevent employee benefits (including group insurance) from being offered to men but not to women and vice versa and stop a group health insurance plan from requiring different premium contributions from males and females.

Outside of the workplace, the rules regarding gender-based discrimination in insurance are a bit of a hodgepodge that depend on both the state in question and the kind of insurance being sought. A few states prohibit practically any form of gender-based differences in the offering of insurance and even prohibit the common practice of charging different gender-based amounts for life insurance. Other parts of the country prohibit gender discrimination in the offering of some forms of insurance (such as health insurance) but not others. A third faction of states puts percentage-based limits on gender-based pricing but doesn't outlaw the practice entirely. Before the Affordable Care Act put an end to gender discrimination in the pricing of health insurance in the individual market in every state, more than half of the individual states didn't limit gender-based pricing for individuals.

Insurance Discrimination Against Men

As a society, we've come to view gender discrimination as an issue that mainly has a detrimental impact on women. However, some major forms of alleged insurance discrimination have resulted in men paying more than their female counterparts. In most states, it is still widely accepted that men will pay more for life insurance because of their shorter life expectancy and the shorter amount of time that an insurer will be able to profit from their premiums.

Similarly, in areas where auto insurers are allowed to make gender-based decisions, men tend to pay more because of their greater accident history. The difference in pricing is especially pronounced among young drivers, with insurers apparently assuming that young males will be more reckless behind the wheel than young females.

Insurance Discrimination Against Women

Historically, insurance discrimination against women has mainly been an issue in the health insurance market. When gender-based pricing has been allowed, females have generally paid more for health insurance than males.

To people with only basic knowledge of health insurance, the increased cost for covering women might seem like a byproduct of pregnancy and various maternity-type expenses. Indeed, childbirth and prenatal care are expensive. But since those kinds of care have historically been excluded from individual health

insurance policies (as opposed to group plans) or only covered through the addition of an expensive rider, they don't entirely explain why health insurers in the individual market have usually given women higher rates.

Regardless of their child-bearing capacity, women have traditionally been charged more for individual health insurance products because they utilize medical services on a more frequent basis than males. Particularly through age 55, women are more likely to visit their doctors, receive preventive services and use prescription medications. As men and women approach senior citizenship, costs begin to even out across gender lines, with older men eventually using more care than older women.

Women who have obtained their health insurance through a group employer have been protected for decades from having to pay more for coverage than their male colleagues. With the implementation of the Affordable Care Act, it became illegal for health insurers to charge women more even if they were purchasing their own medical insurance and weren't part of a group plan. At the time this course was being written, federal law didn't prevent women from being charged more for other forms of accident and health insurance (such as long-term care insurance), although some states were considering outlawing the practice or had already done so.

Maternity Care

The high cost of childbirth has been a problem for many women, including some who already have insurance. Historically, policies purchased in the individual market didn't need to cover maternity care, and those offering some coverage would limit it to certain circumstances. Women who delivered via a non-elective caesarian section might have had some insurance protection, but those who had normal vaginal births often had to pay thousands of dollars completely out of pocket. In either case, there frequently were no benefits pertaining to prenatal tests and treatments unless special financial arrangements were made in advance.

Coverage for maternity care has been much more widely available to women in group health insurance plans. In 1978, Congress enacted the Pregnancy Discrimination Act, which clarified that discrimination against pregnant women was an illegal form of gender discrimination under the Civil Rights Act of 1964. As a result, health insurance plans for businesses with more 15 employees had to cover maternity care and had to do so on a level equal to other medical services. The requirement provided pregnancy coverage to enrolled employees and to their enrolled spouses.

The passage of the Pregnancy Discrimination Act has often left employers wondering whether the law requires them to cover some controversial kinds of care. Abortion coverage must be provided under this law, but only to the extent that the procedure is necessary to preserve the life of the mother. Regulators and courts have gone back and forth regarding whether the law requires plans to cover contraception. In 2000, the Equal Employment Opportunity Commission—which enforces several labor-related laws on the federal government's behalf—ruled a plan covering other preventive services (such as screenings, immunizations and physicals) must also cover medically prescribed contraception. Similarly, some courts have argued that excluding prescribed contraception is discriminatory because it is used entirely by women and because the health-related effects of contraception disproportionately impact females. More recently, some judges have ruled otherwise, arguing that as long as a plan doesn't cover male-targeted contraception, it doesn't need to cover female-targeted contraception.

The Affordable Care Act addressed pregnancy issues in several ways. In 2014, the requirement to include coverage of maternity care was extended to smaller group plans and to policies in the individual market. Federal regulations also now require non-"grandfathered" health plans (including group plans and policies in the individual market) to cover certain kinds of preventive care without applying copayments, deductibles or coinsurance fees to them. (Grandfathered plans, in general, are individual and group health plans that already existed on March 23, 2010, and that haven't undergone significant changes since then.) FDA-approved contraceptive services for women are considered a form of covered preventive care under the regulations. A limited exemption allows some religious organizations to avoid paying for contraception coverage, but their impacted employees still be offered the coverage at no cost by their insurance company. (At the time this course was being written, some employers and religious groups were challenging the law's contraception requirements at various levels of federal court.)

Plans and policies offering maternity-related benefits must also comply with the Newborns' and Mothers' Health Protection Act of 1996. This federal law was enacted to eliminate "drive-through deliveries," in which new mothers and their infants were discharged prematurely from hospitals for insurance reasons. The law applies to practically all kinds of health insurance, including group plans from an insurance company, self-insured plans created by employers, and policies offered to applicants in the individual market.

Under the Newborns' and Mothers' Health Protection Act insurers covering vaginal births must pay for at least two days of hospitalization for the mother and child. For caesarian births, the requirement is three days. An insurer can still impose deductibles, copayments and coinsurance fees, but cost-sharing can't differ from day to day. For example, if a policy requires a 20 percent coinsurance fee for the first day of hospitalization for a vaginal birth, the fee can't increase for the second day. Mothers are entitled to the coverage regardless of whether they've had their hospital stay certified or approved in advance by their insurer. However, the insurer is allowed to impose higher cost-sharing requirements if certification or approval is not obtained.

By the time the Newborns' and Mothers' Health Protection Act went into effect, most states had already passed similar legislation. Depending on where they live, mothers and their babies might be entitled to additional insurance-related rights.

Domestic Abuse

Some insurance shoppers have complained that they have had problems with insurance companies because of domestic abuse. To some companies selling life, health, disability and property insurance, victims of domestic abuse have been viewed as higher risks. In the life, health and disability markets, the victims might be viewed in a negative light because their relationship history suggests the potential for physical harm. In a broader sense, some companies have believed that victims who stay in abusive relationships lack a certain level of personal responsibility, which could hint at the way they take care of themselves and their property.

Domestic abuse has also created some claims-related issues that have pitted insurers' ethics against their contractual obligations. Suppose a married couple purchases a house and obtains a homeowners policy for the dwelling and its contents. A year later, they experience serious marital problems, with one spouse moving out of the home but remaining a co-insured party on the homeowners insurance policy. In an attempt to harass the spouse who still lives in the home, the other spouse commits vandalism at the property. Since the vandalism was committed intentionally by someone who is covered by the policy, the insurer might be legally capable of denying the victimized spouse's vandalism claim. (Rules vary by state.) But would this be the ethical thing to do?

In another scenario, imagine a case in which a fearful victim with children is weighing the possibility of reporting an abusive spouse to authorities. Since the victim is already undergoing financial strain, he or she is concerned that an insurer who learns about the domestic abuse will use it as an excuse to raise the victim's premiums. Might this concern about insurance sway the victim's decision and serve as a reason to remain in the harmful relationship?

Alleged discrimination against abuse victims received greater attention in the 1990s, when, according to news reports from McClatchy Tribune Business News, the U.S. House Judiciary Committee found that half of the country's top 16 health insurers took domestic violence into account as part of their underwriting processes. Since then, most states have enacted laws and rules that restrict this practice in some form.

Marriage Discrimination

Society has tended to view marriage as a symbol of stability, and insurance companies have tended to agree. Where laws have permitted them to do so, insurers have sometimes provided cheaper insurance to applicants who have a spouse. At times, the assumption is that married couples are more family-oriented than single people, which supposedly makes them more responsible in certain aspects of their life. Unnamed sources have gone a step further and proposed that married couples deserve to pay less because they seem less likely to engage in insurance fraud. But for whatever the reasons, insurers in some states have been known to charge married couples less for auto insurance.

In health insurance, marriage is often in issue with regard to employee benefits. Many businesses with health plans will offer enrollment to employees' spouses, although company contributions for spousal coverage are often either less than the amount paid for employees or non-existent. In recent years, many companies have instituted spousal exclusions in their health plans and have either prevented spouses from joining at all or have put certain conditions on spousal enrollment. For example, as detailed in benefit trade publications like HR Magazine, a group plan might exclude spouses who are eligible for health insurance at their own jobs or might require an additional premium contribution from a spouse who doesn't want insurance through his or her own employer but wants to enroll in a spouse's plan.

Sexual Orientation

As acceptance of gay and lesbian families has increased, employers and health insurance professionals have often responded by choice or by law. Even before same-sex marriage started expanding to several states, a majority of Fortune 500 companies were offering insurance benefits to their employees' same-sex partners.

At first, businesses catered to their gay or lesbian workers by offering group health insurance enrollment to domestic partners. Eligibility and enforcement tended to vary in this regard. In communities where domestic partnerships already existed as a matter of local civil law, companies could verify a partner's eligibility through government documents. In other cases, partners would be eligible for enrollment by affirming that they'd lived together for several years and were sharing their money in a manner similar to a married couple.

At the time, the general reasoning was that domestic-partnership benefits were a way to help gay and lesbian employees who lacked the legal ability to obtain spousal coverage. Ironically, this attempt to address perceived discrimination against one group of workers occasionally caused employers to ponder if their solution actually amounted to discrimination against a second group. Whereas some companies continued to reserve domestic-partner benefits for gay and lesbian partners, others decided to give unmarried heterosexual couples the same chance to enroll in group plans. In cases where domestic-partner benefits were made available regardless of sexual orientation, opposite-sex couples often accounted for the majority of enrollments.

With the passage of civil unions and the introduction of same-sex marriages in many states, health insurance benefits for gay and lesbian partners became less of voluntary issue and more a matter of law. In general, in accordance with various U.S. Supreme Court rulings, couples in a same-sex marriage are entitled to the same insurance benefits as married opposite-sex couples.

HIV/AIDS

By the time AIDS became a matter of public knowledge, thousands of Americans had already been infected with the disease. While scientists and medical professionals struggled to understand how the AIDS virus impacted the body, people who were diagnosed as being HIV-positive were essentially being given a death sentence. Even with the best treatments that were available at the time, a newly diagnosed patient could reasonably expect to live no more than a few more years.

The spread of AIDS created an opportunity for insurance professionals who viewed life insurance as a potentially versatile asset. A new segment of the industry started offering "viatical settlements," in which AIDS patients were offered lump sums in exchange for selling their life insurance to investors. When the patient died, the investors collected the death benefit.

Advances in AIDS treatments have since made it possible for HIV-positive people to live relatively healthy lives for several decades and have made viatical settlements less common. Meanwhile, some AIDS activists have pressured life insurance companies to examine recent AIDS-related data and rethink their approach to HIV-positive applicants. If an applicant is HIV-positive but does not have any of the manifested symptoms of AIDS, should the person automatically be denied life insurance? If an applicant is not HIV-positive but engages in protected sexual activity with an HIV-positive spouse, should the HIV-negative person be issued a policy? Readers who are interested in the answers to those questions for compliance purposes are encouraged to research the health insurance regulations in their specific state.

Credit Scoring

Since the 1990s, companies specializing in personal lines property and casualty insurance have been criticized for basing rates and underwriting decisions, at least in part, on consumers' credit histories.

Practically all insurers who take credit history into account, according to the Federal Trade Commission (FTC), do it for new potential customers who are applying for a policy. Some, but not all, of these companies will evaluate a policyholder's credit again (and make pricing adjustments) when coverage is up for renewal.

According to a comprehensive report from the FTC, the first major system for evaluating insurance customers on the basis of credit was introduced in 1993 by Fair Isaac and Company (FICO), which had already developed similar systems for mortgage lenders and other creditors. Eventually, other companies started offering similar services, and some insurers have since created their own systems.

Although credit history is generally a reflection of someone's tendency to pay bills, insurers don't use this data to judge whether a consumer will pay premiums on time. Instead, they use it to get a broad picture of a person's risk potential and the likelihood of the person actually making insurance claims. Even among critics of this practice, the data, so far, has been very clear that there is a strong correlation between negative credit history and high claim frequency. According to a 2004 study from the Texas Department of Insurance, people with low credit scores filed three times as many auto and homeowners insurance claims as people with high scores. The state also found that credit history was an even better predictor of future auto insurance claims than a person's driving history. In a similar report commissioned by the Iowa Department of Insurance, researchers from St. Ambrose University said, "[T]he current evidence for the predictive power of insurance credit scoring is overwhelming."

Insurers have stressed the correlation between credit scores and claims, but they haven't been consistent in explaining why the correlation exists. In fact, when a State Farm insurance spokesperson was asked by the Daytona Beach News Journal why credit scores are such a good predictor of insured losses, the answer was a succinct, "We don't know why." When pressed for an explanation (either on the record or privately), other insurance professionals have posed the following hypotheses:

- People with bad credit have less disposable income and are less likely to self-insure for relatively small losses, which means they will make more insurance claims.
- People with bad credit have less disposable income and, therefore, are less likely to maintain their vehicles and homes in ways that might prevent certain losses.
- People with bad credit lack personal responsibility and are more likely to put themselves in risky situations.
- People with bad credit may be experiencing financial difficulties and, therefore, might be tempted to commit insurance fraud.

While the first two items on that list might seem logical, the last two are viewed as offensive to some consumers and might explain why the public has resisted the use of credit information in insurance. Some critics point out that bad credit isn't necessarily a sign of carelessness, especially in cases where financial problems are caused by medical issues or widespread unemployment. Others don't care what the statistics say and simply have a problem believing that personal finances should have any impact on how an insurer perceives their driving ability. Insurers have already decided that certain data (such as the different life expectancies across racial groups) should be disregarded as a matter of principle. So, should the link between credit and claims (no matter its strength) be treated in a similarly dismissive way?

To a somewhat lesser extent, insurers' use of credit information to set rates has raised concerns regarding discrimination against minority groups, especially black and Hispanic consumers. The aforementioned report from the Texas Department of Insurance found that those two minority groups had lower credit scores on average and that they "tend to be over-represented in the worse credit score categories and under-represented in the better credit score categories." The report from the FTC reached similar conclusions, but neither report recommended an end to credit-based insurance decisions. Insurers claim that accusations of discrimination are illogical in regard to credit scoring because credit reports do not contain information about race, ethnicity or even income.

Despite the public's misgivings about the use of credit information in insurance, insurers say that most consumers benefit from this practice and receive lower premiums as a result of it. According to a 2004 report from the Florida Insurance Council, eliminating credit from insurers' underwriting and rate-setting criteria would have increased family premiums for auto and homeowners insurance by more than $200. A report cited in the state's Daily Record newspaper found that complaints to the Maryland Department of Insurance actually increased after the state prohibited the use of credit information.

Practically all states have implemented restrictions on the use of credit information in insurance, but those restrictions aren't identical across the country. Whereas some states prohibit the practice mainly in auto insurance transactions, others extend it to property insurance as well (or vice versa). Some allow credit information to be considered for new customers but not existing ones. A few states, such as California, ban the use of credit information in practically all cases. Others, such as Illinois, allow its use but prohibit insurers from using it as the sole factor for taking adverse action (such as a rate increase) against a consumer. In states where use of credit information is allowed, insurers might still need to consider special cases of financial difficulty, such as when bad credit is caused by medical hardship or job loss.

Age

Age is an accepted, significant factor in the offering and pricing of life insurance. After all, the older a person is, the greater the chance of death. But as people grow older, they might also have different experiences paying for health or casualty insurance.

The Affordable Care Act aimed to level the cost of insurance for people regardless of their individual health status. At the same time, though, lawmakers understood that the utilization of health care increases as patients grow older. So while individual health status can generally no longer be used to discriminate against someone who is purchasing major medical insurance, insurance companies are still permitted to charge older people more than younger people. The disparity between rates for young people and older people might be limited to a specific ratio by either federal or state law.

In casualty insurance, age-related discrimination has been alleged by younger drivers (who tend to get into the most accidents) and elderly drivers (who tend to be involved in more fatal crashes). Some auto insurance companies will decrease the cost of insurance for older drivers who complete special refresher courses.

Treating employees differently based on age within a group insurance plan may be possible in some cases. But a thorough review of state and federal employment laws should be considered prior to the implementation of any age-based requirements.

Dog Breed

Along with covering the contents and structure of people's dwellings, homeowners insurance provides financial protection to property owners who are held liable for various accidents. According to 2008 figures from the Insurance Information Institute, approximately one-third of homeowner liability insurance claims resulted from dog bites, and, as reported by the Palm Beach Post newspaper, the average amount of those dog-related claims was a massive $25,000.

In order to guard against the risk of dog-bite insurance claims, some carriers have implemented internal policies that make it more difficult for owners of certain breeds to obtain affordable homeowners insurance. Those policies have been known to be particularly strict in regard to their treatment of pit bulls.

For owners of pit bulls, the breed-related restrictions can prompt some tough choices. Some owners have reported being denied insurance from multiple companies because of their dog and have needed to secure coverage through their state's typically more-expensive FAIR plan. Others admit to lying about their dog's breed in order to keep their family pet without experiencing financial penalties. Insurance worries have even had an impact on animal shelters and rescue services. In Minnesota, one pet adoption organization told the local Star Tribune newspaper that roughly one-sixth of adoption applications are withdrawn by potential dog owners in anticipation of insurance problems.

The alleged discrimination against certain breeds has been criticized, particularly in cases where consumers are denied insurance or charged more even though their pet has no history of violence. A few states have banned the practice, and several others have debated the issue over the past decade or so.

Travel Plans

U.S. consumers who apply for life insurance have sometimes experienced underwriting problems when they've revealed plans to travel to certain countries. When these problems arise, they often involve areas of the Middle East, such as Israel and Palestine, or third-world countries that are locked in a civil war. Many states have enacted rules that either prohibit or limit travel plans from being used to deny insurance or to increase someone's premiums.

Conclusion

Opinions about insurance-related discrimination have evolved over time and have sometimes challenged our understanding of what is fair or unfair. In order to remain solvent and protect themselves from major losses, insurance companies must analyze risk very carefully. But in order to maintain positive relationships with customers, they must be aware of how the public views their methods of offering and pricing certain products. Above all else, even when insurance professionals believe that a particular person or a particular group should be treated differently in regard to pricing or availability of coverage, they must be mindful of anti-discrimination rules from federal and state governments. Ethical concerns about discrimination can be handled by examining various facts and applying them to our unique value systems. Questions of law should be referred to appropriate experts to ensure full compliance.

CHAPTER 3: HIPAA PRIVACY COMPLIANCE

Introduction

In the mid-1990s, members of Congress generally agreed that health care needed to be administered more efficiently and that delivering it would be simpler if there was a set of national standards for doctors and insurers to follow when handling electronic transactions. But just imposing those standards and encouraging greater utilization of electronic health records wouldn't be enough to please patients and providers.

The concept of the internet was still relatively new to many Americans, and even those who were fine with sending some data through computer networks weren't entirely comfortable with the possibility of their medical information being intercepted by hackers and identity thieves. If the government wanted sensitive information to be shared in new ways, it would need to ensure that people's privacy would remain intact.

Congress tackled those basic concerns on a bipartisan basis by passing the Health Insurance Portability and Accountability Act of 1996, known more simply as "HIPAA." Full implementation of HIPAA was delayed at first by a rush of public comments about the law and then by changes in leadership at the U.S. Department of Health and Human Services in the years that followed. But by the middle of the first decade in the 21st century, anyone who was providing or receiving medical services was feeling the effects of one our country's most significant privacy laws.

General Overview of HIPAA

So, what exactly did HIPAA do? A detailed answer to that question is what this course is all about. But as a starting point, here are some of the areas in which HIPAA has had the greatest impact:

- Thanks to HIPAA, new employees and their dependents have the right to join an employer's group health plan regardless of their health status.
- Thanks to HIPAA, people who are insured through a group health plan can be covered for pre-existing medical conditions after a special waiting period has passed.
- Thanks to HIPAA, there are uniform procedures for doctors to follow when billing electronically for treatment.
- Thanks to HIPAA, purchasers of long-term care insurance can receive federal tax breaks.
- Thanks to HIPAA, doctors and health plans generally can't disclose a patient's medical information without the person's consent.
- Thanks to HIPAA, most doctors and health plans are required to take security-related measures to keep medical information safe.

Our focus here will mainly be on the last two of those points.

Noncompliance with HIPAA's privacy rules has created unfortunate situations involving either one of two extremes. On one hand, there have been examples of medical personnel being completely ignorant of the rules by posting people's x-rays on social networking websites and selling celebrities' medical information to gossip publications. However, there have also been instances in which a doctor or nurse has leaned too heavily on the law and prevented a patient's loved ones from receiving important information in an emergency. In between those extremes, there are countless cases of professionals who have wanted to do the right thing but have been unsure about what HIPAA allows or prohibits.

Throughout this chapter, we'll try to give you a strong background in your rights and responsibilities under the law in a wide variety of common situations. In some cases, you might be surprised to read about protections you didn't know existed. Alternatively, you might discover that some broad exceptions to these rules leave you with fewer protections than expected.

A Disclaimer About This Chapter

As you review the following information about privacy and security requirements, please be advised that the totality of all HIPAA-related rules could fill several hundred pages. So while you'll find plenty of information here, a course like this can't possibly address all the details and all the nuances that exist in the actual law and regulations. If you're working with clients and have access to their health information, we strongly suggest you review HIPAA thoroughly on your own or at least consult an expert who is familiar with your specific situation.

Health Information Privacy Rules

To provide and pay for health care in relatively simple ways, certain people need access to your medical information. If you don't tell your doctor about your medical history, you might end up being misdiagnosed. If your doctor doesn't share information about you with your insurer, he or she might not be compensated for treatment.

Still, most patients seem to agree that details about your health are your own business and should only be disclosed on a need-to-know basis. Since you probably wouldn't want everyone in the world to know what surgeries you've had and what medications you've taken, you expect your physicians to protect your privacy as much as possible.

Laws regarding medical privacy existed before HIPAA, but they were mainly enacted on a state-by-state basis. Through a collection of regulations known as the "Privacy Rule," HIPAA created national standards that dictate what doctors, insurers and other collectors of medical data can do with your information. Those standards also determine your right to access your own medical records, as well as your right to correct errors in them.

The authors of the Privacy Rule attempted to promote a balance of confidentiality and efficiency in the health care system. On one hand, they recognized that patients put a lot of trust in their doctors and expect their personal records to be guarded with care. Yet they also knew putting too many restrictions on the sharing of information could slow the system down and prevent patients from getting treatment in a timely fashion.

Whether the authors ultimately succeeded in finding that balance has been a source of heated debate in the medical community. But no matter which side of the debate you're on, you'll probably agree that complying fully with the Privacy Rule isn't easy. If you aren't careful and well-informed when medical information is being shared, someone's rights could be at risk. Those rights, of course, can include your own.

Kinds of Protected Health Information

HIPAA doesn't allow certain entities (mainly health care providers and health insurance plans) to use or disclose specific medical information about you unless you give your consent or unless the use or disclosure is allowed by the Privacy Rule. This specific medical information is called "protected health information."

One of trickiest parts of HIPAA compliance is figuring out what exactly qualifies as protected health information. The Privacy Rule and HIPAA itself can make this task difficult because they contain many similar terms and definitions. For example, along with the term "protected health information," the Privacy

Rule also has separate definitions of “health information” and “individually identifiable health information.” We can’t understand HIPAA’s requirements unless we know what those terms really mean.

To be considered “health information,” the information must have all of the following traits:

- It is created by or given to a health care provider, a health plan, a public health authority, an employer, a life insurance company, a school or university or a health care clearinghouse.
- It relates to a person’s past present or future medical condition, genetic information, health care provided to a person, or the past, present or future payment of health care for a person.

That definition, though, is just a starting point. Health information, in and of itself, is not the kind of information that can’t be used or disclosed without your consent. In fact, some of the entities mentioned in that definition (such as life insurance companies and schools), generally don’t need to follow the Privacy Rule.

Health information isn’t protected by the Privacy Rule unless it is considered “individually identifiable health information.” To be considered “individually identifiable health information,” the information must have all of the following traits:

- It is created by or given to a health care provider, a health plan, an employer or a health care clearinghouse. (Note the absence of life insurers, schools and public health authorities from the definition.)
- It relates to a person’s past, present or future medical condition, health care provided to a person, or the past, present or future payment of health care for a person. (Note that this trait is also part of “health information.”)
- It either identifies the person or could reasonably be used to identify the person.

That last point is key to HIPAA compliance. A doctor who says something like, “I once treated someone for tuberculosis,” wouldn’t necessarily be violating the Privacy Rule. But a doctor who clarified that statement by saying, “I once treated Jane Smith for tuberculosis,” could be in some legal trouble. With this in mind, information that would normally not seem medical in nature (such as your name, your Social Security number and your address) can be “individually identifiable health information” if it is disclosed along with information about your health, your treatment or your payment for treatment.

The same standard would apply in regard to information about payments for health care. While a health insurer might be within its rights to tell a news reporter, “We’ve paid over $5 million in claims this year,” it might be a violation of HIPAA to say, “The policyholder at 123 Main St. has made a $5,000 claim.”

But even then, the information might not be considered “protected health information” and, therefore, might not be subject to the Privacy Rule. In general, “protected health information” is “individually identifiable health information” that is transmitted or stored in any way. However, “protected health information” typically doesn’t include information from school records or employment records.

So, why is there a distinction between “individually identifiable health information” and “protected health information”? The short answer is it helps clarify how employers need to follow the law. If you haven’t already, you’ll soon understand that certain entities need to comply with the Privacy Rule while others don’t. Someone who is exempt from the Privacy Rule doesn’t need to keep your protected health information confidential.

Employers are in a unique position in that they are generally exempt from the Privacy Rule when acting strictly as your boss but not necessarily exempt when they are acting as the sponsor of your group health plan. Don’t be too concerned if this sounds confusing at first. We’ll elaborate on the distinction between employers and plan sponsors in a little while.

Now that you know that “protected health information” is basically “individually identifiable health information” with a few exceptions, let’s go over some important details by answering some questions.

Does it Matter How Information Is Transmitted or Recorded?

An important element of HIPAA known as the "Security Rule" only applies to information that is stored electronically. However, the Privacy Rule applies to individually identifiable health information in all its forms. The information can be stored electronically, written by hand or spoken.

What Are Some Basic Kinds of Information That Are Protected?

Examples of information protected by the Privacy Rule include:

- Information you discuss with your doctor, a nurse or other health care provider.
- Information in your medical files.
- Information about health insurance claims.
- Information about medical bills.
- Non-medical information (such as your name, address and phone number) if it can reasonably be used to identify you and help people learn something about your health.

Is Information About Relatives Protected?

Information doesn't have to be about you in order to be protected. If you give your doctor some details about your parents' medical history, the doctor needs to treat those details as protected health information. The doctor generally can't disclose them without your consent.

What About Information That Predates HIPAA?

HIPAA's Privacy Rule is retroactive, meaning it protects information that doctors and health insurers currently possess but obtained prior to the law's passage. It doesn't matter, for example, if you were treated for leukemia way back in 1960. The information is still protected.

Even the deceased retain some HIPAA rights for several years after their death. We'll have more on that topic later.

When Can Protected Health Information Be Shared?

Someone who must follow the Privacy Rule can't share protected health information unless the law provides an exception or you give your consent.

Applicability to Covered Entities

With just a few important exceptions, the only people or entities that need to follow the Privacy Rule and keep your information confidential are "covered entities." A covered entity can mean any of the following:

- A health care provider.
- A health plan.
- A health care clearinghouse.

As you can see, that's a relatively limited list. If you're concerned about your privacy in general, keep the brevity of this list in mind when discussing your medical information with anyone. Though it wouldn't be the nicest thing to do, your neighbor can gossip with others about your medical history and not be in violation of HIPAA. Businesses that get a hold of your medical information might not be obligated to keep it private if they aren't involved in providing or paying for health care.

Still, each item on the list of covered entities deserves some clarification.

Health Care Providers

We tend to associate the phrase "health care provider" with doctors. But the true definition of the word is a bit broader and incorporates many other people. According to the Department of Health and Human Services, a provider might be any of the following:

- A doctor.
- A hospital.

- A clinic.
- A pharmacy.
- A dentist.
- A psychologist.
- A chiropractor.
- A mental health center.
- A nursing home.

Providing medical services to patients doesn't necessarily make a person a covered entity. A health care provider is exempt from the Privacy Rule if it never shares health information electronically. Examples of providers who might be exempt from the Privacy Rule include those who don't do electronic billing, don't electronically inquire about patients' insurance coverage and don't electronically authorize referrals. But since most providers do these things (and since there is still no exemption if a provider relies on a third party to do them), there are very few providers who can ignore the Privacy Rule.

Although the electronic transmission of information helps determine if a provider has to follow the Privacy Rule in the first place, it doesn't change the kind of information that is protected. Once it has been established that a provider is a covered entity, that provider must keep all protected health information confidential, including information found on paper and information revealed in conversation. The information doesn't need to be stored electronically for it to be covered by the Privacy Rule.

Again, be careful not to confuse HIPAA's Privacy Rule with HIPAA's Security Rule. Unlike the Privacy Rule, the Security Rule only pertains to electronic information. You'll read about the Security Rule later in this course.

Health Plans

A health plan is basically defined as an individual plan or group plan that pays for health care. Common examples include the following:

- Health insurance companies.
- Health maintenance organizations (HMOs).
- Company health plans.
- Government health plans, including Medicare and Medicaid.

As usual, there are some important details to consider when trying to figure out exactly which health plans need to follow the Privacy Rule.

Is the Privacy Rule Only for Group Plans?

No matter if it sells insurance in the group market or the individual market, a health insurer is a covered entity under the Privacy Rule. This is a big difference compared to HIPAA's rules about portability and nondiscrimination, which often don't apply to the individual market.

Are There Major Exemptions for Health Plans?

Some self-insured health plans are not covered entities and generally don't have to worry about the Privacy Rule. In a self-insured health plan, an employer sets up a mechanism whereby it is responsible for paying employees' medical bills. In a true self-insured plan, coverage for employees is not purchased from an insurance company.

A self-insured health plan is not a covered entity under HIPAA if it has fewer than 50 participants.

What If an Insurer Doesn't Share or Receive Information Electronically?

In the rare event that a health insurance company doesn't share or receive information electronically, it still must obey the Privacy Rule. The exemption regarding electronic information and providers doesn't extend to health plans.

What About Other Kinds of Insurance Companies?

A common misconception about HIPAA is that life insurance companies are covered entities and need to follow the Privacy Rule. The Department of Health and Human Services has concluded that life insurance companies and workers compensation insurers generally aren't governed by the rule. The confusion regarding this issue is understandable because life insurers and other non-health insurers often collect medical information about their customers.

Still, don't assume the Privacy Rule doesn't factor into the way these insurers do business. When a life insurance company decides that it will only sell you a policy after reviewing your medical records, those records typically can't be shared with the company unless you have signed a HIPAA-compliant authorization form. Though the insurer technically still wouldn't be a covered entity at that point, the authorization form might put contractual restrictions on how the company can use your information.

Keep in mind, too, that many life insurance companies have branched out into the health insurance market by offering traditional health insurance, long-term care insurance and other health-related coverage. In its role as a provider of this coverage, an entity calling itself a "life insurance company" might actually be a health plan under the law.

Also, be aware that our focus here is strictly on HIPAA. Even in cases where other types of insurers might not technically be regulated by that law, various other laws (including at the state level) might require those carriers and their agents to follow strict privacy rules.

Health Care Clearinghouses

According to the Department of Health and Human Services, health care clearinghouses are entities that take health information in a non-standard format and put it in a standard format or vice versa. Health care clearinghouses rarely have direct relationships with patients, but they play important roles during the health-care billing process.

Applicability to Employees

You may have noticed that most examples of covered entities (with the exception of some health care providers) technically aren't individuals. With this in mind, you might wonder how employees of covered entities fit into the Privacy Rule. If a doctor improperly discloses protected health information but is employed by a hospital and isn't involved at all in things like electronic billing or insurance inquiries, who is at fault? Would the covered entity (the hospital) be liable for the disclosure, or would the employee (the doctor) be the one in trouble?

How about a customer service representative at an insurance company? Since the representative isn't a health plan on his own, would the representative be in legal trouble if he didn't keep a customer's information confidential?

Those questions weren't clearly addressed in HIPAA's original form, and the officials in charge of enforcing the law sometimes couldn't agree on the answers.

Congress tried to clear up some of the uncertainty by passing the HITECH Act in 2009. Under the act, an employee who takes or discloses personal health information from a covered entity without proper authorization has violated HIPAA.

Applicability to Business Associates

Whether they realize it or not, some businesses and individuals aren't covered entities but are still indirectly expected to uphold the Privacy Rule. Many of these businesses and individuals are known as "business associates."

Business associates are third parties that are given protected health information in order to provide services to a covered entity. They aren't members of a covered entity's workforce, but they might find themselves acting on a covered entity's behalf.

Examples of potential business associates include:

- Lawyers representing covered entities.
- Health insurance agents and brokers.
- Transcription companies for health care providers.
- Third-party administrators for health plans.
- Third-party billing companies for health care providers or health plans.
- Accountants working with covered entities.

Business associates are impacted by the Privacy Rule through "business associate agreements." A business associate agreement is a contract between a business associate and a covered entity. It explains what the business associate can and can't do with protected health information. The agreement can't allow the business associate to do anything that the covered entity wouldn't be able to do under the Privacy Rule. It can even force the associate to agree to rules that a covered entity wouldn't have to follow.

Until 2010, business associates were only indirectly regulated by HIPAA. Though they couldn't do anything that violated the Privacy Rule, they technically couldn't be charged with HIPAA violations. If you were a business associate and improperly disclosed someone's health information, the victim might've taken legal action against the covered entity that gave you the information. Then, the covered entity might've responded by suing you for violating your business associate agreement. But in the end, the federal government wouldn't have subjected you to any HIPAA-specific penalties.

Like it did for employees of covered entities, the HITECH Act expanded liability under HIPAA to include business associates. If you are a business associate and violate a business associate agreement, you generally can face the same legal consequences as a covered entity.

Here's some additional guidance to help you understand the relationship between covered entities and business associates.

What If a Business Associate Violates the Law?

Upon becoming aware of a possible HIPAA violation, the covered entity is required to notify the business associate. At that point, depending on the severity and the continuance of the violation, the covered entity might need to help fix the problem or terminate the business associate agreement. The same actions must be taken by business associates if they are aware of violations by covered entities.

Do Covered Entities Need to Have Agreements With All Third Parties?

Business associate agreements are only for third parties who receive or access protected health information from a covered entity. If a covered entity deals with a vendor who doesn't receive or access protected health information, the vendor doesn't need to sign a business associate agreement.

There's also not necessarily a need for a business associate agreement under HIPAA if it is technically possible for a third party to access protected health information but very unlikely for it to occur. For example, under limited circumstances, a shipping company or post office might be allowed to accept a package containing protected health information without having to sign an agreement.

What Happens When Agreements Expire?

If a business associate agreement expires or is terminated, the business associate must do one of the following:

- Return the protected health information to the covered entity.
- Destroy the protected health information.
- If the information can't be returned or destroyed, agree to keep the protected health information private.

Do Covered Entities Need Agreements When Sharing Information With One Another?

Covered entities generally don't need to sign business associate agreements when they share information with one another for the purpose of billing or treating people. If your doctor decides to get the opinion of a colleague about your health, your information might be shared with the other doctor without the need for an agreement. Your doctor is also typically allowed to share your information with your insurer in order to be paid for medical services.

If information is shared among covered entities for other reasons, a business associate agreement might be required. According to the Department of Health and Human Services, an outside physician who is hired to train hospital employees would need to sign a business associate agreement before accessing patients' information as part of the training.

What If a Business Associate Decides to Outsource Tasks and Responsibilities to Another Business?

On occasion, protected health information might be given by a business associate to a subcontractor or other entity as a way of completing a business task. For example, an insurance broker might give paper versions of protected information to a shredding company in order for the information to be destroyed.

If protected health information is provided by a business associate to a subcontractor or other entity in order to perform business tasks, the subcontractor or other entity will also be considered a business associate. Therefore, the subcontractor or other entity must abide by the Privacy Rule and any contractual requirements it has agreed to. However, the covered entity who provided information to the first business associate is not responsible for having a business associate agreement with the subcontractor or other entity and is not responsible for ensuring the subcontractor's or other entity's compliance. Instead, the business associate who gives protected health information to another business associate must obtain reasonable assurances that the information will be protected. In most cases, this will be accomplished by having the two business associates enter into a business associate agreement. The agreement between the two business associates must be at least as strict as the agreement between the first business associate and the covered entity that provided or will ultimately receive the protected health information.

Applicability to Plan Sponsors

"Plan sponsors" are indirectly required to follow parts of the Privacy Rule in certain situations.

A plan sponsor is the entity that arranges for people to join a group health plan. In the majority of cases, it's an employer who decides to have a health plan for employees or a union that decides to have a health plan for its members.

HIPAA affects plan sponsors because it puts limits on the kinds of information they can receive from their health plans. It also restricts what sponsors can do with the information once they receive it.

A sponsor usually can't receive protected health information from a health plan unless it signs a special agreement. The agreement will state what the sponsor can and can't do with the information, and it can't let the sponsor do anything that would otherwise be a violation of the Privacy Rule. The agreement will also forbid the sponsor from using the information to make employment-related decisions. (Decisions regarding whether to change or discontinue a group plan are allowed.)

You'll read more about plan sponsors in the section "Sharing Information in the Workplace."

Parties Exempt From the Privacy Rule

Since we've spent so much time going over who is a covered entity and who isn't, it's worth revisiting the basics before moving on to our next topic. Again, with a few exceptions, the Privacy Rule only needs to be followed by covered entities. The list of covered entities is limited to the following:

- Health care providers who engage in certain electronic activities.
- Health plans.
- Health care clearinghouses.

Since HIPAA was enacted, many people have incorrectly assumed that the number of covered entities is larger than those three. Even though they may receive health information on a regular basis, the following entities generally aren't covered entities:

- Life insurers
- Workers compensation insurers
- Property and casualty insurers
- Schools (assuming they don't provide health care on a regular basis and don't engage in certain electronic transactions).
- Law enforcement officials.

But don't forget the main point of the Privacy Rule: A covered entity can't share your protected health information with a non-covered entity unless you or the rule allow it. So while non-covered entities aren't necessarily limited in the ways they can share your information, they may be limited in the ways they can receive it.

Required Authorization and Consent Forms

HIPAA allows covered entities to use or disclose protected health information without your permission in any of the following circumstances:

- The use or disclosure is designed to help treat you.
- The use or disclosure is designed to ensure payment for medical services.
- The use or disclosure is part of "health care operations." (Health care operations are an assortment of tasks that are integral to running a reasonably efficient covered entity. An example would be training employees at covered entities to use computer systems.)

Using or sharing information for other reasons generally can't be done without your consent. The Privacy Rule requires that consent be provided through the use of an authorization form. The form has several mandatory elements to it, and it must be used even if you are the one requesting that information be shared with someone.

Among other things, a HIPAA-compliant authorization form needs to contain all of the following items:

- The kind of information that will be used or shared.
- The person or entity that will be using or disclosing the information.
- The person or entity that will be receiving the information.
- The deadline for the receiving entity to receive or access the information.
- Information about your right to cancel the authorization and how to exercise that right.
- Whether allowing the use or disclosure will affect your right to treatment or insurance benefits.
- Disclosure of the fact that the information might not be protected by the Privacy Rule once it has been shared.
- A place for the date and your signature.

Let's go over some common questions about authorization forms.

Does the Form Need an Exact Expiration Date

Authorization forms need to mention how long the receiving party can access or receive your protected health information. They don't need to contain an exact date.

For example, if access or disclosure will be allowed on a continuing basis, the form can mention this in place of a deadline. It's also acceptable to use a particular event (such as the end of a medical research study) instead of a specific date.

Does the Government Require the Use of Specific Language in the Form?

The language in an authorization form can be written entirely by the covered entity. The government only requires that it contain the required information and be understandable.

How Do Consumers Remember What's in the Form?

When you sign an authorization form, you are supposed to receive a copy from the covered entity.

Can a Form Allow Covered Entities to Disclose Future Information?

Authorizations can be made ahead of time. If you want someone to receive copies of all your future medical records, you can authorize it by signing a single form.

Permissible Use and Sharing of Protected Health Information

Covered entities can use or share protected health information without your authorization if the use or sharing is done to facilitate treatment, payment or health care operations.

Early drafts of HIPAA regulations didn't allow this to happen, but it was ultimately decided that requiring authorization in these situations would be impractical and potentially harmful to patients. If you were to become very sick and needed immediate medical attention, you'd probably want medical professionals to have easy access to your past and present health records. If you were having important tests done, you'd probably want your doctor to be able to access those tests and report back to you as soon as possible without having to get your signature on something.

You can request that a covered entity not share your information for the purpose of treatment, payment or health care operations, but the covered entity doesn't need to grant your request. Still, if you make the request and the covered entity agrees to it, the entity must stick to the agreement.

Suppose you're concerned about identity theft and don't want your Social Security number shared with anyone. You might ask your doctor to keep the number private, but the doctor might need the number to receive payment from your insurance company. Since this kind of sharing relates to payment, the doctor might be allowed to refuse your request and disclose the information to your insurer.

These exceptions to the rules about authorization can be very helpful to covered entities, but it's important not to read things into the exceptions that aren't really there. For example, a doctor's right to share information with a business associate for treatment purposes doesn't mean a business associate agreement isn't required.

Also, keep in mind that the exceptions about authorization relate to the covered entity's right to use the information on its own or share the information with a third party. They technically don't give the third party a right to obtain the information, even when treatment, payment and health care operations are involved.

As an example, if your new doctor contacts your old doctor and requests protected health information for treatment purposes, your old doctor isn't required to share it. If he or she wants, the old doctor can refuse to disclose the information until you've signed an authorization form.

In most situations, the only person who can't be denied access to your personal health information is you.

Treatment

Covered entities generally don't need your authorization to use or share your information for treatment purposes. This allows a health care provider to go through your medical records in order to give you appropriate medical advice. It also lets one provider share your information with another provider so you can get the best care possible.

Disclosures for treatment purposes can sometimes be made to people who aren't medical professionals. Perhaps the most common example of this would be a disclosure of your health status to a friend or family member in an emergency situation. Another would involve allowing a pharmacist to give medicinal information to someone who picks up a prescription for you. In both examples, the relative, friend or other person might be thought of as being involved in your treatment or responsible for it. (There are, however, many restrictions on situations like these. We'll analyze these scenarios again later.)

Treatment can also include contacting patients about appointments and care. But since emails and voicemails can sometimes be accessed by someone other than the intended recipient, many providers are hesitant to leave messages. After all, a statement as simple as “My name is Dr. Smith, and Mary Jones is one of my patients” could be a HIPAA violation, depending on the reason for saying it.

HIPAA doesn’t prevent your doctor from leaving you a message, even if the message is left with another person. What matters are what is said and why. If the intent is treatment-related (such as to confirm an appointment or go over your test results), a message of some kind is allowed. A message would also be allowed if it relates to payment or health care operations.

It might be impossible for the doctor to avoid disclosing some protected health information in the message (such as your name and the fact that you’re a patient), but that’s not a HIPAA-related problem if the disclosure is as limited as possible.

So, if the message is meant to confirm an appointment, the doctor might say the scheduled time but not disclose the reason for the visit. If the doctor is trying to reach you to discuss a medical issue, the message might simply say to call the provider’s office.

If you’re concerned about communication from a covered entity falling into the wrong hands, you can request that covered entities only contact you in certain ways (such as only by phone or only at a certain number). As long as your preference is reasonable, the covered entity needs to honor it.

Payment

Covered entities can use or disclose your protected health information to ensure they are properly paid for their services. This allows doctors to send your information to your health plan and vice versa. If someone else is responsible for paying your medical bills, your information can be given to them, too.

The HITECH Act created some new restrictions in regard to payment-related disclosures. To properly understand them, we should briefly recall some basics about disclosures to covered entities.

In general, a covered entity can share information with another covered entity without authorization if the sharing is done for reasons of treatment or payment or health care operations. Even if you ask a covered entity not to engage in this kind of sharing, the entity doesn’t need to honor your request.

As of 2010, you can ask your doctor not to share information with your health plan for purposes of payment or health care operations, and the doctor must agree if you pay for treatment entirely out-of-pocket. This consumer protection is expected to be utilized by patients receiving particularly personal kinds of care, such as abortion services and treatment for sexually transmitted diseases.

Health Care Operations

Covered entities can use and disclose protected health information while conducting health care operations.

The term “health care operations” is probably one of the most difficult HIPAA concepts to grasp. It’s an admittedly vague phrase but is generally used to describe reasonable activities that would be expected to be done at a covered entity. Some major examples include employee training and the underwriting of health insurance (by an insurance company).

For clarity’s sake, here’s the exact definition from the Privacy Rule:

Health care operations means any of the following activities of the covered entity to the extent that the activities are related to covered functions:

(1) Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; patient safety activities (as defined in 42 CFR 3.20); population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment;

(2) Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities;

(3) Except as prohibited under §164.502(a)(5)(i), underwriting, enrollment, premium rating, and other activities related to the creation, renewal, or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance), provided that the requirements of §164.514(g) are met, if applicable;

(4) Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;

(5) Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and

(6) Business management and general administrative activities of the entity, including, but not limited to:

(i) Management activities relating to implementation of and compliance with the requirements of this subchapter;

(ii) Customer service, including the provision of data analyses for policy holders, plan sponsors, or other customers, provided that protected health information is not disclosed to such policy holder, plan sponsor, or customer.

(iii) Resolution of internal grievances;

(iv) The sale, transfer, merger, or consolidation of all or part of the covered entity with another covered entity, or an entity that following such activity will become a covered entity and due diligence related to such activity; and

(v) Consistent with the applicable requirements of §164.514, creating de-identified health information or a limited data set, and fundraising for the benefit of the covered entity.

Incidental Disclosures

The authors of the Privacy Rule understood that preventing every single kind of unauthorized disclosure would be impossible. Whether patients and policyholders like it or not, some protected health information is inevitably going to be available to complete strangers.

Covered entities aren't expected to prevent this sharing from happening at all costs. They just need to protect it in reasonable ways and implement common-sense safeguards.

Minor disclosures that occur despite reasonable actions by covered entities are known as "incidental disclosures." These disclosures are either accidental or practically necessary to facilitate treatment, payment or health care operations. They're bound to happen from time to time, and they aren't examples of HIPAA violations.

Our previous discussion of phone messages and email ought to help you understand incidental disclosures. If your doctor leaves you a message on your answering machine and you play it when someone else is in the room, the disclosure of your health information to the other person is considered incidental. If your doctor or insurer communicates with you via email, the covered entity likely wouldn't be in trouble if you open up a message and the text is seen by someone looking over your shoulder.

Other incidental disclosures commonly occur at hospitals and medical offices. Within reason, a provider can call out your name in a waiting room without violating HIPAA, and your doctor can discuss your health with you even if you're sharing a hospital room with another patient.

In another example, a nursing home or hospital might be allowed to put your name by the door to your room. The fact that visitors can see it is outweighed by the way it makes treatment and health care operations simpler for the covered entity.

The Minimum Necessary Rule

HIPAA sometimes grants covered entities the power to use and disclose protected health information without consent, but that power is far from absolute. Even in cases where use or disclosure is allowed, the covered entity needs to follow the "minimum necessary" standard.

Under the minimum necessary standard, protected health information can only be used or disclosed to the extent that the information is needed to complete a task allowed by HIPAA. In other words, if only a portion of your information is needed to do a particular act, a covered entity should only share that portion and keep the rest confidential.

The minimum necessary standard might be best understood by considering how providers share information with health plans. If you visit your doctor for a broken leg, the doctor can send protected health information to your insurance company for billing purposes. This disclosure is allowed without your authorization since it relates to payment. But since things like your weight, your blood pressure and your family's medical history probably aren't needed for the insurer to make payments for a broken leg, your doctor isn't supposed to share them.

Similarly, while a psychologist might need to share a general diagnosis of your mental health with your health plan, disclosing the specifics of what you discuss in therapy would likely violate the minimum necessary standard.

The minimum necessary standard is about more than just disclosures to outside individuals. It also controls how information can be accessed or shared within a single covered entity. To comply with the standard, a covered entity needs to identify all of the following:

- The people within the organization who will have access to protected health information.
- The kinds of personal health information that those people will be able to access.
- The circumstances under which those people will be allowed to access the information.

To demonstrate how this might work, let's think of a family doctor working out of a small office. The doctor might determine that her office assistant (but not her office's janitorial and maintenance staff) ought to have access to patients' protected health information. Then she might decide that the assistant should only be able to access patients' contact information, basic insurance information and their general reason for making appointments. Finally, the doctor might believe that the assistant should only be allowed to access the limited amount of protected health information in order to make appointments, make insurance inquiries and prepare visitors for examinations.

Based on the doctor's decisions, the assistant would be following the minimum necessary standard if he accessed a patient's general information to confirm an appointment. But let's assume one of the assistant's close friends came in for treatment, and the assistant accessed the friend's health records out of personal curiosity and concern. In that case, the assistant wouldn't be abiding by the standard.

Right to Your Own Information

A law mandating privacy of your information wouldn't be very significant if you didn't have a way of knowing what your information actually contained. For all its focus on disclosures to third parties, HIPAA still gives you several rights involving access to your own records. These rights include:

- The option to receive copies of your medical records.
- The option to correct errors in your records.
- The option to know if your information is being shared without your authorization.
- The option to let a friend or family member control access to your records.

Let's take a closer look at each of those rights.

Obtaining Copies of Medical Records

You have a right to know what pieces of information a covered entity has about you. Probably the easiest way to find out is to contact the entity and request a copy of your protected health information.

You can receive a copy of any protected health information that has been recorded by the covered entity and included in a "designated record set." (Keep in mind that information you convey in conversations might not be recorded and, therefore, might not apply to this portion of the Privacy Rule.) The Privacy Rule defines "designated record set" in the following manner:

Designated record set means:

(1) A group of records maintained by or for a covered entity that is:

(i) The medical records and billing records about individuals maintained by or for a covered health care provider;

(ii) The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or

(iii) Used, in whole or in part, by or for the covered entity to make decisions about individuals.

Covered entities are required to give you a copy of your protected health information if you request one. Even if you have unpaid bills from the covered entity, you still have a right to the information. A covered entity can't charge you anything for the copy, other than the reasonable cost of labor, postage and supplies that are associated with the copying.

The rules about cost apply to you and a person known as your "personal representative," but some covered entities have been known to charge more when information requests come from third parties, such as attorneys and insurance companies. (We'll go into detail about personal representatives later.)

In general, you're supposed to receive a copy of your information within 30 days after making a request. A one-time, 30-day extension is possible if proper notice is given to the person making the request.

You can have your records given to you in any form that is reasonable for you and the covered entity. For example, you might receive them in the mail, via fax or in an electronic format if the covered entity is set up to provide them in those ways. However, under the HITECH Act, if your records are stored electronically by the covered entity, they must be made available in an electronic format to you as well.

There are very few occasions when a covered entity can turn down your request for your records. An example would be a request for copies of psychotherapy notes. These notes don't need to be shared if a therapist doesn't store them in your medical records.

If a covered entity is refusing a request for your records, it might be because the request is coming from your personal representative rather than from you. Your personal representative is very similar to someone who has medical power of attorney and is often a family member who is responsible for your health care.

Your personal representative has the general right to access your protected health information in the same way you do, but a covered entity might determine that disclosing certain information to the person isn't in your best interest. This sometimes occurs when a physician suspects a personal representative of committing spousal or child abuse.

If a covered entity denies you or your personal representative access to your information, you can appeal the entity's decision. In this case, the decision to share your records or keep them confidential will often be made by an impartial health care provider.

Making Changes to Medical Records

If you access your protected health information within a designated record set and notice an error, the covered entity that gave you the information is responsible for correcting it. Errors usually need to be fixed within 60 days after a request, but covered entities can get a 30-day extension if they give notice to the consumer.

After a covered entity has corrected the records in its possession, it may be required to send the changed data to other companies and individuals. At the consumer's request, corrected information must be given to anyone who has received the person's protected health information from the covered entity and who would reasonably benefit from knowing about the correction.

Sometimes, a consumer and a covered entity will disagree about whether information is accurate and whether a change should be made. If a covered entity doesn't believe an error exists, it can refuse to make a correction. The denial must be stated in writing, along with the reason for the denial and an explanation of how the consumer can file a complaint. At your request, the fact that you are disputing the accuracy of the information must be added to your records.

Accountings of Disclosures

When covered entities disclose your protected health information, they are required to keep records of the disclosure. These records must be made available to you if you request them.

At your request, you can receive information about these recorded disclosures if they were made in the previous six years. The information must be given to you within 60 days after your request and generally needs to include the following:

- Who received your disclosed information.
- What information was disclosed.
- When the disclosure occurred.
- Why the disclosure was made.

Let's answer a few questions about the tracking of disclosures.

Is Information About Disclosures Free to Consumers?

You can request a free accounting of disclosures once each year. If you make additional requests, you might have to pay a reasonable fee.

Are Covered Entities Required to Maintain Protected Health Information for a Set Period of Time?

HIPAA doesn't force covered entities to keep your protected health information for any length of time. It only requires that they keep records of disclosures.

Rights of Your Personal Representative

Nearly the same rights that you have under HIPAA (including the right to receive your information, correct errors in it and authorize disclosures of it) also belong to your "personal representative." Your personal representative is anyone who has the legal right to make health care decisions on your behalf.

By default, the person who can make medical decisions on your behalf is determined by state law. For most children, the person would be a parent. For most married adults, it would be a spouse, and for most unmarried adults, it might be a parent, a sibling or a grown son or daughter. By signing power-of-attorney documents, you can designate someone as your representative regardless of state law.

The rights given to personal representatives can be extremely important because they can be used to give loved ones critical information in serious situations. For example, if you are your elderly mother's personal representative and she goes in for emergency surgery, you can access her medical records before making difficult treatment decisions for her. If you are the one in serious condition and are incapacitated, you can rest assured that timely and informed choices about your health can still be made by someone close to you.

Since they tend to be utilized in emergency situations, the rights of personal representatives should be made clear to patients and providers sooner rather than later. Answers to the following questions might come in handy at the right time.

Can a Covered Entity Refuse to Give Information to a Personal Representative?

As you'll note later in this course, covered entities have the option to share your information with your family and friends without your authorization, but they aren't required to do it. The opposite is true regarding your personal representative.

Because your personal representative is acting in your place, a covered entity generally can't refuse to give the representative access to your protected health information. A rare exception would be a case in which the entity believes giving information to your representative would reasonably result in harm to you. In practice, this exception is used when you are in danger of being physically abused or neglected by your representative.

However, depending on the law and various agreements that you may have entered into, someone can be your personal representative in one situation but not in others. If the specifics of a situation mean that the person doesn't have the right to make a particular medical decision for you, the person isn't your representative and can't control or use your information. This point is clarified in answers to the next few questions.

Is the Same Person My Representative Whenever I'm Incapacitated?

Whether someone's role as a personal representative applies to all cases of incapacitation will depend on what state law says and what extra legal protections you've put in place. If you've gone beyond state law and delegated medical decision-making to another person in limited situations, that person is only your personal representative in those limited situations.

For a practical example, imagine you have gone beyond state law and given your best friend the power to make decisions about life support. Your other medical decisions will be made on your behalf by your sister.

In this example, your best friend would only be your personal representative if a decision needs to be made about your life support. If you aren't on life support but are otherwise incapacitated, your friend wouldn't be your representative and wouldn't be able to access your information. On the other hand, your sister would be able to access your information in the second case but not the first.

Can Someone Be My Personal Representative If I'm Not Incapacitated?

Someone is your personal representative when they have the legal right to make health care decisions for you. Unless you or a court make some unconventional arrangements, this right is only given to someone if you are physically or mentally incapable of making your own choices. If you want someone to receive your information but aren't incapacitated, you might need to sign an authorization form first.

An exception to this rule allows parents to access a child's protected health information even if the child can think and communicate. Since there are other special guidelines for the use and disclosure of children's information, we'll address this issue in another section.

Do Non-Medical Powers of Attorney Make People a Representative?

You can arrange for someone to make financial decisions on your behalf, but that alone doesn't make the person your personal representative. Unless the person has the power to make health decisions for you, a covered entity isn't required to give the person your information without your consent.

You'll recall, however, that covered entities have the option (not the obligation) to share your information without consent for the purpose of payment. If you are responsible for paying your father's bills, his insurance company can send you his financial statements without violating HIPAA.

Sharing Information in an Emergency

There's hardly a more important time to understand HIPAA than in an emergency.

Suppose you're with your brother who suddenly collapses. You rush to the emergency room and are told to wait outside by yourself while the medical staff tries to revive him. An hour later, you finally track down a doctor. But when you ask the physician about your brother, she refuses to give you any information. She tells you that since you aren't your brother's personal representative, she can't tell you anything about his

condition, including where he is or how he's feeling. After all, she says, giving you that kind of information without your brother's authorization would violate HIPAA.

The outcome of our hypothetical story is generally in conflict with HIPAA. Though a health care provider might have an internal policy that prevents employees from giving information to a patient's loved ones, HIPAA doesn't prohibit this form of sharing.

If you are not available to give your consent or if you are incapacitated, a covered entity can share some of your protected health information with family members and close friends. Covered entities are allowed to disclose information under these circumstances if they believe doing so is in your best interest and that you probably wouldn't object to it. Based on their professional judgment, they can share information in these situations to the extent that the recipient is involved in your care.

So getting back to our example, it's reasonable to assume that giving you information about your brother's condition would be in his best interest. (Even if you aren't the one who can make medical decisions for him, you might be in charge of contacting the person who fits that description.) And since you were the one who made sure he got to the hospital in the first place, you've become involved in his care. While the doctor would be out of line if she were to tell you information that didn't relate to your brother's collapse, HIPAA still allows her to give you some information about his current condition.

The same standards apply to information shared over the phone. If you have an accident and aren't capable of telling medical personnel who to contact, your doctor or your hospital can use professional judgment to contact a friend or family member on your behalf. The covered entity doesn't need to worry about whether the contacted person is your personal representative.

If you are available to your health care provider, your information can be shared with friends or family if the provider believes doing it would be in your best interest and you don't object. So if you are in the emergency room but are still competent and able to communicate, your doctor can simply say something like, "I'll go tell your son what's going on." By saying nothing to stop the doctor, you might be giving him consent to share at least some of your information with your son. You might not need to sign an authorization form for this type of sharing.

Sometimes your consent can be implied. For example, if you invite someone into a treatment area while you are being examined, your provider might be allowed to infer that talking about your condition in front of that person is acceptable.

Here are some other situations in which a covered entity might be able to use professional judgment and disclose some of your protected health information without your consent to friends or family:

- Someone is picking you up from treatment and would benefit from knowing how to transport you safely.
- Someone is going to be looking after you while you are sick or injured and would benefit from knowing how to keep you safe or provide basic treatment.
- Someone is helping you pay your medical bills and needs protected health information for financial reasons.
- Someone is picking up medication for you and would benefit from knowing about dosages, side effects and other drug-related matters.

Because this aspect of the Privacy Rule is so important yet so misunderstood, we'd be foolish if we didn't explore it in greater detail.

Are Covered Entities Required to Share Information With Friends or Family Members in Emergencies?

HIPAA gives covered entities the option of sharing your information with these people without your authorization. However, covered entities aren't obligated to share your information with anyone other than you or your personal representative.

Health care providers might have internal policies that prevent your friends and family members from receiving any protected health information under any circumstances. These policies are generally allowed, but they aren't required by HIPAA.

How Is My Personal Representative Different From Other Friends and Family Members?

Your personal representative can act on your behalf to make medical decisions and take several actions in regard to your protected health information. This person can access all of your protected health information, request amendments to it and authorize disclosures of it on your behalf. Practically the only time a covered entity can refuse to give information to your representative is when there is a reasonable chance that the representative will abuse you.

Other friends and family members don't have any rights to your information under HIPAA. Without your authorization, they can't access your information unless a covered entity believes disclosing it would be beneficial to you. The covered entity can pick and choose what to tell these people about your health status, and unless they're your personal representative, they can't amend your records or authorize disclosures. They can't make medical decisions for you.

Sharing Information in the Workplace

Despite not being covered entities, employers deal with HIPAA indirectly when they act as "plan sponsors."

A plan sponsor is essentially any entity that decides to create a group health plan for itself. A sponsor can choose to fund its group's health care independently (in an arrangement known as self-insuring), or it might decide to purchase coverage for the group from a health insurance company.

A plan sponsor's involvement in HIPAA compliance will depend on how its plan is structured and what information the sponsor receives from the plan. If an employer offers its plan entirely through an insurance company and only receives a limited amount of health information from its insurer, its participation in HIPAA compliance won't be particularly complicated. (In this case, the employer's insurance company will probably be charged with handling HIPAA's administrative requirements.) But if the employer is self-insuring, it will be at least partially responsible for ensuring that its plan is following HIPAA's many privacy requirements.

Before going into too many specifics about different kinds of health plans, we need to emphasize that there are plenty of situations in which medical information provided at work has nothing to do with HIPAA. Even as the Privacy Rule regulates the instances in which your health plan can give information to your employer, it doesn't always stop your employer from getting your information from other sources and using it inappropriately.

In general, HIPAA has little or no power over information that companies obtain in their role as employers. For example, when you request a medical leave of absence, your employer can require that you give a reason for your request. When you attempt to take a sick day, your supervisor can still demand to know why you won't be in the office.

Since medical information in those situations would be coming from you rather than from the health plan, your company would be receiving it as an employer, not as a plan sponsor. Nothing in HIPAA would force your employer to keep your medical information private in either of those examples. (Of course, your employer might be required to follow other laws that restrict the use or disclosure of your information. For simplicity's sake, we'll only concern ourselves with HIPAA requirements here.)

Similarly, since it would need the information for payroll purposes, your employer can receive information about whether you are enrolled in its plan and how much of your paycheck is supposed to be earmarked for premiums. And though your doctor might not be allowed to disclose the results of a drug test to your employer without your consent, you might still be turned down for a job if you don't let your employer access the information.

Fully Insured Plans vs. Self-Insured Plans

HIPAA compliance can be relatively simple for employers when they sponsor a fully insured plan. A fully insured plan is a group health plan in which coverage is secured entirely through an insurance company or HMO. The opposite of a fully insured health plan is a self-insured plan, in which the employer pays members'

medical bills partially or entirely on its own. In general, self-insured plans are more popular among large employers than among small employers.

Since employers are usually the ones who sponsor health plans, it's easy to assume that they are responsible for keeping their plans HIPAA-compliant. But if an employer sponsors a fully insured plan and its insurer doesn't give the employer any information about employees other than enrollment information and "summary health information," most of HIPAA's administrative responsibilities will be handled by the insurance company.

Summary health information is health information about the benefits provided under the employer's plan, including the plan's claims history. This information may disclose the kinds and costs of treatment that group members have received, but it won't include data that can be used to identify a particular employee, other than five-digit ZIP codes. A plan sponsor can only receive summary health information (without members' consent) for limited purposes, such as shopping around for lower premiums and making changes to its health plan.

Fully insured plans that don't let employers access other information generally just need to ensure that their plan doesn't retaliate against people for exercising their HIPAA rights and doesn't force members to waive any of those rights. Other administrative duties can be handled by the employer's insurance company.

To keep this straight in your mind, you might find it helpful to view these kinds of plans as two separate plans. One plan is at the employer level and is the employer's responsibility. Another plan is at the insurer's level and is the insurer's responsibility. For the fully insured arrangements that we've been discussing, the administrative requirements for the plan at the employer's level are minimal.

If a plan is self-insured or lets the plan sponsor receive protected health information other than enrollment and summary health information, the sponsor will have more responsibilities. Even though the employer would still technically not be a covered entity, the portion of its business that is administering the health plan would be acting as one. As a covered entity, this portion of the employer's business needs to do the following:

- Not retaliate against employees for exercising their HIPAA rights.
- Not force people to waive their HIPAA rights.
- Create and maintain a privacy notice.
- Provide the privacy notice to group members in the manner described in the section "HIPAA Privacy Notices." (If the plan is fully insured but receives or creates protected health information besides enrollment and summary health information, the notice only needs to be provided upon a member's request.)
- Appoint a privacy officer who will be in charge of keeping the health plan compliant with the Privacy Rule.
- Create internal privacy policies that address who can access or use protected health information, what information they can use or access, and the circumstances under which use or disclosure will be allowed.
- Have a written or electronic copy of its internal privacy policies.
- Establish a process for members to file privacy complaints.
- Implement safeguards to prevent unauthorized or unintentional uses and disclosures.
- Train employees to follow privacy practices and procedures.
- Require third-party administrators and other service providers to sign business associate agreements before obtaining protected health information from the plan.

If a health plan is going to be sharing information with its sponsor besides enrollment and summary health information, the legal documents establishing the plan must be amended. Among other things, the following points must be made clear in the amended documents:

- The sponsor can't use or disclose protected health information in ways that are prohibited by the plan documents.
- Any agent acting on the sponsor's behalf must follow the same privacy rules as the sponsor.
- The sponsor needs to contact the plan if it knows of any improper use or disclosure of protected health information.
- If possible, the sponsor needs to get rid of or return protected health information when the information is no longer needed.
- The sponsor can't use protected health information to make employment-related decisions.
- The sponsor will only allow certain people to access protected health information on its behalf. (These people must be identified in the plan documents.)

Understand that this is only a summary of a plan's main requirements at the employer level. For additional requirements impacting employers and other plan sponsors, see the Privacy Rule.

Exemptions for Some Group Plans

Though HIPAA's rules about insurance portability and nondiscrimination still need to be followed, the Privacy Rule doesn't apply to self-insured health plans with fewer than 50 participants. Group plans that only offer life insurance, disability insurance or some other non-health kind of coverage are also exempt.

Using Information for Marketing Purposes

Covered entities can't use or disclose your protected health information for marketing purposes without consent. A covered entity is marketing to you if it is communicating with you about a product or service and encouraging you to purchase or use the product or service. A covered entity is also generally forbidden from selling your information to a third party, including situations in which the third party just wants to market to you.

There are, however, some cases in which a covered entity can promote goods and services and not be marketing to you. For instance, no marketing is going on (and no authorization is required) if a covered entity is promoting a product or service as part of legitimate treatment. If you phone your doctor and complain of certain symptoms, your doctor generally can recommend a particular drug to you as a way of relieving those symptoms. Also under HIPAA, marketing is not necessarily going on when a covered entity is using your information to promote a health-related product or service that it provides.

A covered entity doesn't need your authorization before marketing products and services to you in a face-to-face conversation or when giving you a small promotional gift.

Marketing Rules Under the HITECH Act

Through the HITECH Act, Congress tightened and clarified the HIPAA marketing rules for covered entities and their business associates. Among other things, the law added the following rules:

- If a covered entity or business associate is disclosing your protected health information in exchange for compensation, the authorization form that you sign must state whether the party receiving the information can resell it.
- If you receive communication from a covered entity for the purpose of fundraising, you need to have a way to opt out of future fundraising communications.

Even if a covered entity is marketing products or services to you that are provided by that entity, your authorization might still be required. Much will depend on whether a third party is paying the covered entity to do the marketing. (As an example, think of a health plan that's being paid to advertise a particular benefit, or a doctor who's being paid by an equipment manufacturer to market certain procedures to all patients.)

Sharing Information With the Government, the Courts and Other Authorities

There are plenty of times when government authorities and courts could benefit from having protected health information. The information might help the government detect illegal activity, assist people in defending themselves, or assist local health officials in the containment of infectious diseases.

Covered entities can disclose your information to the government, the courts and other authorities without your authorization. We'll summarize how these disclosures are allowed, but be aware that the Privacy Rule has many specific requirements that will depend on a given situation. If you find yourself in a position where you feel obligated to give health information to a lawyer, a government representative or a police officer, you'll probably want to review the Privacy Rule first or speak with an attorney.

The Government

Covered entities can give your protected health information to the government if the information is required by law. They might also share your information as a way of cooperating with regulatory investigations.

The Courts

Whether information can be shared as part of a lawsuit will depend on who's involved in the suit and who's asking for the data.

Covered entities can disclose protected health information if they are a plaintiff or defendant and the information relates to their case. If you are suing your doctor for malpractice, the doctor generally doesn't need your permission to use your medical records as part of a defense. If your health plan has taken legal action against you for nonpayment, your payment information can be used against you without your consent.

When they aren't plaintiffs or defendants, covered entities can share information without your consent in accordance with a judge's order. When a judicial request is made by a party other than a judge, covered entities might be allowed to share your information without your consent in either of the following situations:

- The covered entity or the person requesting the information has made a reasonable attempt to contact you and given you a reasonable chance to object to the disclosure.
- A court has issued a protective order that sets privacy restrictions on your information.

Law Enforcement

Law enforcement entities occasionally use protected health information to prevent and solve crimes. Here are a few instances in which sharing information with law enforcement would generally be allowed:

- The sharing is required by law.
- The sharing is done to protect someone from immediate harm.
- The sharing is requested by law enforcement to help identify or locate a criminal. (The Privacy Rule has special limits on the kind of information that can be shared in this scenario.)

Public Health Authorities

Covered entities can share your information with a health authority if the disclosure is made with the intent of protecting the public. Like most other kinds of disclosures, this sharing still needs to be compliant with the aforementioned minimum necessary rule. In other words, if a piece of information isn't needed to fulfill a particular purpose, it's supposed to be kept confidential.

Other Assorted Privacy Requirements

Regardless of whether any protected health information has been shared yet, covered entities need to comply with the Privacy Rule's administrative requirements. You already read about some of these requirements in the section "Fully Insured Plans vs. Self-Insured Plans."

Other than some fully insured plans at the employer level, all covered entities must follow the Privacy Rule by doing the following:

- Appointing a privacy officer to oversee compliance with the Privacy Rule.
- Providing appropriate privacy-related training to employees.
- Applying sanctions against employees and business associates who violate privacy rules.
- Documenting any sanctions against employees and business associates who violate privacy rules.
- Implementing appropriate safeguards to keep protected health information private.

- Creating a process that allows the public to file privacy complaints.
- Documenting any privacy complaints.
- Creating procedures that minimize the harmful effects of privacy violations.
- Not intimidating, threatening or discriminating against people for exercising their HIPAA rights.
- Not forcing people to waive their HIPAA rights for the purpose of treatment, payment, eligibility for benefits or enrollment in a health plan.
- Keeping a written or electronic copy of privacy practices (for at least six years after they are no longer in effect).

Relationship to Other Privacy Laws

We're just about ready to turn away from the Privacy Rule. But before we do, we ought to reiterate that HIPAA's privacy requirements are minimal standards and aren't the only medical privacy rules in existence.

People who aren't covered entities need to understand that being exempt from HIPAA requirements doesn't exempt them from other laws regarding health information. Covered entities need to know that uses and disclosures that HIPAA allows might be prohibited by other laws. In general, if a law provides greater privacy protection than HIPAA, that law must be obeyed.

Health Information Security Rules

The Privacy Rule isn't the only collection of standards that covered entities need to follow. A covered entity and its business associates also need to comply with HIPAA's Security Rule.

Whereas the Privacy Rule deals mainly with how protected health information can be used or disclosed, the Security Rule addresses how the information needs to be guarded. It contains a number of administrative, physical and technical safeguards that need to be implemented whenever protected health information is stored or transmitted in an electronic format.

Information stored on a server or on a desktop computer is considered to be in an electronic format, and so is data that's stored on a removable disk. Information that's transmitted over the phone or via fax generally isn't in an electronic format.

When it was enacted, the Security Rule was applicable only to covered entities (health care providers, health plans and health care clearinghouses). Because of the HITECH Act, business associates are now required to obey it too.

A business associate's obligation to follow the Security Rule's requirements needs to be part of a business associate agreement. If a plan sponsor wants to receive protected health information in an electronic format, the sponsor must agree to implement a security plan of its own.

Implementing a Security Plan

Ever since it was proposed, the Security Rule has made some covered entities nervous. Under the impression that the rule's requirements are too complicated and costly, many providers and plans remain noncompliant with this part of HIPAA.

In reality, the Security Rule was written with flexibility in mind. The people drafting it understood that no two covered entities are exactly the same and that they all have different amounts of technical and financial resources available to them. The rule is intended to be used as a general set of standards that can be followed at all levels of the health care industry without becoming outdated.

So before diving into too many details, we should clarify some basics about what the Security Rule requires and what it doesn't. Contrary to popular belief, it doesn't force anyone to utilize any particular kinds of software or other computer-related technology. It doesn't even force covered entities or business associates to encrypt electronic health information.

Instead, the Security Rule sets several broad security-related goals and expects covered entities to achieve them in whatever way seems reasonable. In return for being able to choose the specifics of their security plan, covered entities are required to reevaluate that plan if their exposure to security risks ever changes.

When deciding how to implement the standards set by the Security Rule, covered entities are allowed to take the following factors into consideration:

- The covered entity's exposure to security risks.
- The cost of implementing particular security measures.
- The covered entity's existing security measures and how they accomplish the goals of the Security Rule.

Required Safeguards and Addressable Safeguards

The specific safeguards mentioned in the Security Rule are either "required" or "addressable." If a safeguard is required, covered entities must implement security measures that satisfy it. If a safeguard is addressable, covered entities need to at least determine whether the safeguard is reasonable or appropriate for them.

When covered entities believe a Security Rule safeguard is reasonable and appropriate, they need to implement it. When an addressable safeguard isn't reasonable and appropriate, covered entities can ignore it by doing all of the following:

- Documenting that the safeguard isn't reasonable and appropriate.
- Documenting why the safeguard isn't reasonable and appropriate.
- Implementing an alternative safeguard that is reasonable and appropriate.

The required and addressable safeguards are divided broadly into three categories: Administrative safeguards, physical safeguards and technical safeguards. Within those broad categories, you'll often see subgroups of safeguards. These subgroups are known as "standards."

In the next three sections, we've summarized the standards and safeguards and identified which ones are required and which ones are addressable.

Administrative Safeguards

Standard: Security Management Process (Create and implement procedures to protect information, detect security problems and fix security problems.)

- Safeguard: Risk Analysis (Identify the risks to your electronic data and the size of those risks.) REQUIRED
- Safeguard: Risk Management (Take steps to bring your identified security risks down to a reasonable level.) REQUIRED
- Safeguard: Sanction Policy (Create penalties for employees who violate security rules.) REQUIRED
- Safeguard: Information System Activity Review (Regularly monitor the security of information systems.) REQUIRED

Standard: Assigned Security Responsibility (Choose someone who will be responsible for picking and implementing security measures.) required

Standard: Workforce Security (Take steps to ensure that authorized employees can access information and unauthorized employees can't.)

- Safeguard: Authorization and/or Supervision (Implement procedures to determine if people should have access to information and how they should be supervised.) ADDRESSABLE
- Safeguard: Workforce Clearance Procedure (Implement procedures to prevent unauthorized people from accessing information.) ADDRESSABLE
- Safeguard: Termination Procedure (Implement procedures to ensure that once people lose access, it stays lost.) ADDRESSABLE

Standard: Information Access Management (Determine how access to information should be achieved.)

- Safeguard: Isolating Health Care Clearinghouse Functions (If you have a department that acts as a health care clearinghouse, take steps so that information from that department isn't shared improperly with other departments.) REQUIRED
- Safeguard: Access Authorization (Determine how people should be able to access information.) ADDRESSABLE
- Safeguard: Access Establishment and Modification (Document, review and modify [if needed] how access to information is allowed and achieved. ADDRESSABLE

Standard: Security Awareness and Training (Create training for people within the organization.)

- Safeguard: Security Reminders (Keep the workforce appraised of security procedures.) ADDRESSABLE
- Safeguard: Protection From Malicious Software (Protect your system from viruses and similar problems, and train employees about this risk.) ADDRESSABLE
- Safeguard: Log-in-Monitoring (Take steps to monitor situations in which people attempt to access information but don't succeed.) ADDRESSABLE
- Safeguard: Password Management (Make procedures for creating, changing and safeguarding passwords, and communicate password policies to employees.) ADDRESSABLE

Standard: Security Incident Procedures (Decide what should be done when there's an issue with information security.)

- Safeguard: Response and Reporting (Implement procedures for identifying security problems when they occur and minimizing their impact.) REQUIRED

Standard: Contingency Plan (Have a plan for situations in which normal access to information is lost.)

- Safeguard: Data Backup Plan (Make copies of electronic information for emergency access.) REQUIRED
- Safeguard: Disaster Recovery Plan (Have a plan for restoring lost access to information.) REQUIRED
- Safeguard: Emergency Mode Operation Plan (Make sure an emergency doesn't jeopardize the security of information.) REQUIRED
- Safeguard: Testing and Revision Procedures (Periodically test contingency plans, and revise them as needed.) ADDRESSABLE
- Safeguard: Applications and Data Criticality Analysis (Determine which computer programs are most important to the handling of protected health information.) ADDRESSABLE

Standard: Evaluation (Evaluate all security plans periodically to address risks and compliance with the Security Rule.) REQUIRED

Standard: Business Associate Contracts and Other Arrangements (Don't share information with business associates unless you believe they'll keep it protected.)

- Safeguard: Written Contract or Other Agreements (Document a business associate's obligation to keep information safe.) REQUIRED

Physical Safeguards

Standard: Facility Access Controls (Implement procedures that limit access to information and to the facility housing the information.)

- Safeguard: Contingency Access Controls (Have a way to make information secure and/or adequately accessible when a contingency plan is underway. ADDRESSABLE
- Safeguard: Contingency Security Plan (Take steps to address theft, tampering or unauthorized access of electronic information at the facility.) ADDRESSABLE

- Safeguard: Access Control and Validation Procedures (Determine who at the facility should have access to areas where information is accessible.) ADDRESSABLE
- Safeguard: Maintenance Records (Document any repairs and modifications that relate to the physical security of the facility.) ADDRESSABLE

Standard: Workstation Use (Implement policies explaining how devices related to electronic information are to be used, including devices used outside of the facility.) REQUIRED

Standard: Device and Media Controls (Develop policies regarding how information should be received, handled and disposed of on hard drives or portable storage devices.)

- Safeguard: Disposal (Implement procedures regarding how to dispose of information and the items on which it's stored.) REQUIRED
- Safeguard: Media Reuse (Require that media storage devices can't be reused unless old information is deleted from them.) REQUIRED
- Safeguard: Accountability (Document cases in which information is moved from place to place.) ADDRESSABLE
- Safeguard: Media Backup and Storage (Ensure that information has been copied before moving the equipment that stores it. ADDRESSABLE

Technical Safeguards

Standard: Access Control (Create methods and controls to ensure that information is only accessible to authorized personnel.

- Safeguard: Unique User Identifier (Be able to track users of information systems by name or identification number.) REQUIRED
- Safeguard: Emergency Access Procedure (Implement ways for information to be accessible in emergency situations.) REQUIRED
- Safeguard: Automatic Logoff (Use a system that logs people off after an extended period of inactivity.) ADDRESSABLE
- Safeguard: Encryption and Decryption (Figure out how to encrypt and decrypt information.) ADDRESSABLE

Standard: Audit Controls (Implement procedures for recording activity on systems.) REQUIRED

Standard: Integrity (Take steps to ensure information can't be improperly changed or deleted.)

- Safeguard: Mechanism to Authenticate Electronic Protected Health Information (Monitor whether information has been inappropriately altered or destroyed.) ADDRESSABLE

Standard: Person or Entity Authentication (Take steps to ensure that people trying to access information are who they say they are.) REQUIRED

Standard: Transmission Security (Take measures to prevent unauthorized access while information is being transported through a network.)

- Safeguard: Integrity Controls (Make sure information isn't modified or destroyed during transmission.) ADDRESSABLE
- Safeguard: Encryption (Use a system that encrypts data when appropriate.) ADDRESSABLE

Dealing With Security Breaches

The Privacy Rule and Security Rule made covered entities responsible for the proper use and disclosure of protected health information. But until 2009, nothing in HIPAA or its related statutes guaranteed that a victim of a serious privacy breach would ever be alerted to the situation. While some states had laws requiring breach notifications, many others didn't address the issue and let covered entities make up their own minds about whether contacting affected persons was appropriate.

One of the most significant changes brought on by the HITECH Act was the requirement that covered entities notify individuals of security breaches. The law also forces business associates to alert covered entities when protected health information has been used or shared in unauthorized ways.

Regarding HIPAA, breach notifications only need to be made when the wrongfully used or disclosed information was "unsecured." For data that is stored electronically, information generally is unsecured when it has not been destroyed or encrypted. For data stored on paper, information generally is unsecured when it has not been destroyed or shredded.

Under the law, breach notifications are required unless the covered entity can demonstrate that an individual's privacy was probably not compromised. If a disclosure is technically a HIPAA violation but isn't likely to compromise someone's privacy, a covered entity isn't obligated to contact the victim.

When deciding whether a notification is necessary, covered entities are advised to consider both the kind of information that has been breached and the person who gained access to the information. If covered entities determine that notification isn't necessary, they still need to document the unauthorized use or disclosure and their reason for not notifying anyone.

There doesn't need to be proof of a breach for the notification requirement to go into effect. If a situation suggests there might have been a breach, it needs to be treated as though one actually occurred.

Breach Notifications

A notice to an affected individual must contain the following:

- The date when the breach occurred (if known).
- The date when the covered entity became aware of the breach.
- The steps that have been taken to minimize harm to the individual.
- The steps the individual can take to minimize harm.
- Contact information that can be used to find out more about the breach.

Breach notifications need to be made to affected individuals no later than 60 days after a covered entity either knows of a breach or reasonably should have known about it. This includes any time when an employee or agent of a covered entity knew about a breach but didn't report it.

Covered entities can delay notifications if they receive a request from law enforcement. If the request is made orally, an entity can delay notification for 30 days. When the request is in writing, the entity can wait until the time specified in the request. The law allows these delays in order to keep notifications from compromising criminal investigations.

Breach notifications should be made via first-class mail and sent to the individual's last known address. A covered entity can notify people by email if they have already agreed to be reached that way, or by phone if other forms of communication are too slow to prevent harm. If an affected individual has died, the covered entity can send the notice to the person's personal representative or next of kin.

When a breach involves 10 or more people whose contact information is unknown, the covered entity has two options. Notification of the breach to those people can be made on the home page of the entity's website for 90 days, or it can be made through a toll-free telephone number that is active for 90 days. The entity is required to advertise the phone number in the local print and broadcast media.

Breaches that require notifications also need to be reported to the Department of Health and Human Services. Breaches involving less than 500 people in a state or other jurisdiction need to be reported to the government in annual reports within 60 days after each calendar year. For larger breaches, a covered entity needs to notify the government at the same time that affected individuals are given notice, and advertising must be done in print and broadcast media.

Criminal and Civil Penalties

The HITECH Act increased the size of penalties for HIPAA violations and made them applicable to covered entities, business associates and employees. The severity of a penalty will depend on the violator's history of compliance, the violator's knowledge of the law and the violator's intent.

Civil monetary penalties range from $100 for a single mistake to $1.5 million for repeated serious offences. Criminal offences can land a violator in jail for as long as 10 years if the person broke the law with malicious intent or for financial gain.

Conclusion

HIPAA remains an important law for anyone who is concerned about medical privacy. Students who are interested in potential changes to HIPAA should periodically contact the Department of Health and Human Services or visit the department online.

CHAPTER 4: ERRORS, OMISSIONS AND PROFESSIONAL LIABILITY

Introduction

All experienced insurance producers have come to understand that there are universal risks that human beings face every day, including the risks of death, disease, personal injury and property damage. Products that address these risks are discussed constantly within the industry, marketed effectively to the public and detailed extensively in countless texts.

Receiving less attention are those risks that apply to people in certain kinds of situations. The following course material addresses those less-discussed and sometimes less-understood risks, with an emphasis on the insurance needs of business professionals. Students will learn about or be reminded of the various insurance products that are geared specifically toward high-ranking corporate executives, doctors, lawyers, architects and others whose jobs expose them to greater liability risks than the average person. By studying this material, producers will also recall that they, too, are often viewed as professionals who can benefit from solid insurance coverage. The material speaks to those producers who have an interest in errors and omissions insurance or malpractice insurance and contains general overviews of those products.

But as valuable as that information might be, it represents only a portion of what professional liability producers must know in order to do their jobs as effectively as possible. While insurance professionals should obviously be able to understand and explain the products and services that are provided by their industry, they may struggle to succeed if they don't put these products and services into specific contexts and understand how a particular policy may or may not satisfy each professional's unique needs. Producers will probably have a hard time selling a malpractice policy to an attorney, for example, if they don't first grasp what roles an attorney might play in an organization.

With that in mind, the material is as much about the risks encountered by various professionals as it is about insurance products. By applying such important background information to their business interactions with lawyers, doctors and others, producers may become better equipped to match clients with the proper insurance product and may be more apt to recognize major deficiencies in coverage.

Liability Risks for Insurance Professionals

With so much of an insurance producer's time devoted to sales and the management of other people's risks, it is possible for producers to become distracted by daily business tasks and unintentionally ignore the liability risks in their own lives.

This is unfortunate for a number of reasons. On a societal level, a producer who doesn't adequately understand the liability risks within his or her profession could engage in unintentionally negligent behavior that does significant damage to innocent consumers. On a personal level, agents and brokers who don't know how to manage their own professional liability are putting their careers and personal assets at great risk.

Liability insurance for insurance producers, which falls under the category of "errors and omissions" coverage, was relatively uncommon several decades ago. But today's disputes between carriers and

policyholders are often traced by one party or the other to a producer's alleged misconduct, making a quality errors and omissions policy more of a valuable safeguard than in years past.

A producer can be sued if he or she was poorly trained in a policy's features and exclusions and misrepresented those features and exclusions to insureds. Misrepresentations made by the insurance producer may lead to successful legal outcomes for policyholders if the misrepresentation occurred prior to a claim and influenced an insured's choice to purchase a policy. On the other hand, a misrepresentation is a comparatively minor problem, at least from a legal standpoint, if it is made after the policyholder has filed a claim, since the misrepresentation had no bearing on the person's decision to buy the policy in the first place.

Liability and the Producer-Consumer Relationship

In some cases, knowing a policy from cover to cover and being able to answer a prospect's questions will still not be enough to protect an insurance professional when the consumer suffers an uninsured loss. Some courts have ruled that producers have special relationships with their customers, which make insurance producers responsible not only for explaining policy issues and obtaining requested coverage but also for assessing an applicant's risk potential and alerting an insured to coverage gaps. A court might rule that a producer had a heightened duty to advise an insured under the following circumstances:

- There was a long-term relationship between the producer and the insured.
- The producer charged a fee for services in addition to a commission.
- The producer was the insured's lone source for insurance information.

This doesn't mean, however, that producers with a duty to advise are free to make statements and recommend courses of action that are beyond their areas of expertise. Insurance agents can be sued successfully, for example, if the advice they dispense to consumers relates to financial planning as opposed to risk management.

Avery v. Diedrich

On the opposite end of the spectrum is the belief that an insurance producer is not an adviser and should therefore follow through with securing the coverage requested by a prospect, even if the producer disagrees personally with that course of action. Proponents of this belief may even go so far as to argue that there is an implied contract between the producer and the prospect and that a producer's failure to obtain requested coverage for a prospect represents a breach of that contract.

This general idea was addressed in the case Avery v. Diedrich. In the Avery case, a couple inherited property that was insured by a $150,000 homeowners policy and asked an insurance agent to increase coverage on the home to $250,000. The agent, having visited the home, doubted the property was worth that much and said a $100,000 increase on a $150,000 policy might arouse suspicion at an insurance company. The owners agreed to have the home reassessed and to get back in contact once the assessment was completed.

The couple went ahead with the assessment, but no one alerted the agent to this fact until after a fire had destroyed the home at a replacement cost of $250,000. The couple sued the agent and got a favorable ruling from a circuit court, which said the agent should have followed through on the requests for enhanced coverage and was therefore liable for the loss.

On appeal, the Court of Appeals of Wisconsin, District Two acknowledged that state law made agents liable for losses when they agree to obtain coverage for consumers and don't follow those instructions. But the court said an agent isn't liable when a consumer requests coverage and the agent doesn't agree to obtain it.

Liability and Insurer Solvency

Sometimes a producer's liability is tied not to misrepresented or unsuitable policy terms and conditions but to the financial health of the insurance company that issued the policy.

Unfortunately, unforeseen catastrophes, poorly analyzed business plans or some combination of the two can push an insurer into a state of insolvency. When insolvencies occur, policyholders' valid claims might not be paid. A claimant might have to wait several years before he or she is reimbursed for an insured loss, and even then, he or she might only receive a mere fraction of a claim. Policyholders who find themselves in this distressing situation might point their finger at an insurance producer and wonder if the person should be punished for putting them in such a mess.

A court ruled in Higginbotham v. Greer that an agent isn't liable when he or she places coverage in good faith with a seemingly healthy insurer and insolvency occurs at a later date. However, producers might be liable for losses when they knowingly place coverage with a financially shaky insurer that ultimately becomes insolvent.

Liability and Procedural Duties

So far, our exploration of an insurance producer's liability risks has focused mainly on big-picture concepts such as suitability, service and knowledge. These concepts should be unquestionably important to the professional who wants to serve the public admirably and keep legal disputes at a minimum, but the reader shouldn't forget that there are also some procedural aspects of an agent's job that are just as relevant to our liability discussion.

In regard to policy application forms, insurance producers can get into legal trouble if they allow a prospect to merely sign a blank form and then fill in the requested information on their own. If producers receive a completed application and believe it contains an error, they should probably not make any corrections to the document without first checking in with the prospect and the insurance company.

After coverage has been issued, a legally prudent producer should report any known claims to carriers in a timely manner. Coverage that is to be replaced should not be cancelled until coverage under the replacement policy has taken effect.

A Final Note on Producer Duties

Regardless of the specific risk faced by a producer, the reader should be aware that each state might have its own view of what an agent or broker must specifically do or not do. Some states might clarify a producer's advisory relationship with consumers (or lack thereof) within their laws and regulations. Similarly, some states might differentiate the duties of an agent (who generally represents insurers) and a broker (who generally represents consumers). Despite the mentions of specific court cases in these course materials, please understand that they are included merely as examples. You should not assume that those cases are applicable to your duties in your home state.

The Need for Professional Liability Insurance

Having established what some of the major liability risks are for insurance professionals, we ought to state something that every successful insurance producer probably already understands: Merely recognizing that a risk exists doesn't, on its own, make people any less susceptible to unpleasant perils. People who are worried that a certain risk may have a negative impact on their lives need to take the next proactive step and find ways to manage that risk.

As in most of the risks we face in our lifetime, we can reduce our exposure to professional liability by altering our behavior and adhering strictly to various rules. But nothing can guarantee we will avoid all legal problems. A single, uncharacteristically lazy error in judgment can saddle an otherwise upright professional with a guilty verdict from a court, and careful business practices are not always going to help good people pay to defend themselves against others who are intent on filing frivolous lawsuits.

Because mistakes happen and because a consumer's motives and sense of reasonableness can be so unpredictable, professional liability insurance (including errors and omissions insurance) exists as an extra layer of protection for risk-averse businesspersons in many professions and industries.

Aren't Professionals Already Covered?

Most people who could benefit from a professional liability policy don't need to hear an insurance producer go on and on about how insurance, as a general product, can reduce economic hardship during a crisis.

They see the value in insurance and have demonstrated their understanding of risk management by obtaining homeowners insurance, health insurance, life insurance and auto insurance for themselves and their loved ones.

Still, these veteran insurance buyers might need a producer to point out how a professional liability policy fits into and enhances their coverage portfolio. In truth, some prospective customers might be correct when they claim to have no need for professional liability insurance. But their reasoning is probably faulty if it's based on the premise that they are protected from professional liability through their homeowners policy or a commercial general liability policy.

The liability side of a homeowners policy provides almost no protection for a homeowner's business even if the business is operated from the home. While certainly more business-friendly than homeowners insurance, coverage under commercial general liability policies has gotten narrower over the past few decades and is unlikely to protect policyholders when they are negligent in their renderings of professional services.

Obtaining Professional Liability Insurance

If potential buyers recognize the possible need for a professional liability insurance policy, they might next want to know how this product is made available to insureds and what the market for the product is like.

Professional liability insurance is sometimes (but not always) secured for individuals by their company. Insurance producers might be covered for errors and omissions through their agency, and lawyers might be covered for malpractice through their firm. Of course, professionals who are new to a company shouldn't make any assumptions about whether they are automatically covered.

When a company purchases liability insurance for its professionals, it may choose to also include coverage for contracted workers and former personnel in addition to current full-time employees. If a professional is not covered by his or her company or doesn't believe that the company's professional liability coverage is sufficient, that person can shop for an individual policy.

An Assortment of Policies

For simplicity's sake, this course material groups malpractice insurance and errors and omissions insurance together into the broader category of professional liability insurance as often as possible. Yet the reader should keep in mind that an insurance company will probably not underwrite and offer all kinds of professional liability insurance in the same way. A given carrier might feel comfortable giving reasonably priced liability insurance to lawyers but demand that doctors pay comparatively high premiums for malpractice coverage. An insurer that is a leader in errors and omissions coverage for insurance agents might not even have an errors and omissions product on the market that covers architects or engineers.

Such non-uniformity in the liability market probably doesn't come as much of a surprise to readers and is in no way meant to imply that insurance companies are engaging in unethical discrimination toward certain members of the professional world. After all, each professional group presents a unique brand of liability risks to the insurance community. Directors and officers, for example, expose their liability insurers to securities-related liability while not exposing them to many risks pertaining to health issues. The reverse is true for doctors with malpractice coverage. A doctor's liability insurer may have to brace itself for a wrongful death claim but will probably not need to worry so much about a physician getting into trouble with the SEC.

Errors and Omissions Insurance and Malpractice Insurance

Many kinds of liability insurance, including errors and omissions coverage and malpractice coverage, tend to be geared chiefly toward individuals who perform "professional services." Professional services can be defined as work done for clients that requires special knowledge and is usually associated more with intellectual skills than with physical labor.

In general, errors and omissions coverage or malpractice insurance is useful when professional services don't live up to clients' expectations. Client dissatisfaction may be linked to a contract dispute and a professional's alleged failure to render a service as promised, or it might be tied to negligence in the

performance of services. As it applies to professionals, “negligence” may be defined as the failure to act in a manner that would be suitable for a reasonable person with comparable knowledge and skill.

Liability insurance for people who perform professional services will usually cover defense and settlement costs in addition to court-awarded damages. Some policies may also cover legal expenses when a professional hasn’t been named as a defendant in a legal case but gives a deposition in court.

A single errors and omissions policy or malpractice policy will probably not adequately cover a professional who splits his or her time between two dissimilar jobs. Someone who practices law and sells insurance will probably need at least one malpractice policy to cover liability encountered through legal work and at least one errors and omissions policy to cover liability encountered in the insurance business.

When a person has multiple professional roles that are closely related to one another, it may be a bit easier to find desired coverage all in one insurance package. An errors or omissions policy for an insurance agent, for example, might expand coverage so that the agent is also covered when acting as an insurance instructor or as a notary public.

When professionals get their liability insurance through their employer, they might only be covered for the liability they face while working for or representing that particular company. In a hypothetical example, independent insurance agents who only have errors and omissions coverage through their business relationship with Insurer X might only be covered by that insurance while representing Insurer X. When they represent Insurer Y, they might either have no protection under Insurer X’s policy or need to pay a steep deductible in order for Insurer X’s coverage to apply at all to their liability with Insurer Y.

Major and perhaps unexpected coverage gaps are also possible if a policy applies only to “professional acts” and uses a very strict definition of that term. For example, one accounting firm’s errors and omissions policy might be broad enough to protect the company and its employees when someone at the firm makes a costly typing error. However, another firm’s policy might exclude claims related to a typing error because the insurance company doesn’t consider data entry to be something that requires a professional’s skill and intellect.

The importance of understanding what is and is not a professional act can be detected in two real-life court cases: Medical Records Associates v. American Empire and PMI Mortgage v. American International.

Medical Records Associates v. American Empire

In the first case, a company was sued for overcharging a client for copies of medical records. After settling the suit with the client, the company demanded that its errors and omissions insurer indemnify it for legal and settlement costs.

In evaluating the insurance dispute, the United States Court of Appeals for the First Circuit noted that errors and omissions coverage is not meant to be an all-encompassing product that covers all of a professional’s risks, said billing was not a professional service offered by the company and determined that clerical-type errors and omissions were not covered by the company’s policy.

According to the court, “Even tasks performed by a professional are not covered if they are ‘ordinary’ activities ‘achievable by those lacking the relevant professional training and experience.’”

PMI Mortgage v. American International

In the PMI case, a company had been sued for allegedly receiving kickbacks in exchange for giving mortgage companies a good deal on their insurance. The suit had been settled for $10 million, with the company’s insurer — AISLIC — having already advanced roughly $1 million to PMI to cover defense costs and other legal expenses.

According to court documents, the AISLIC policy was supposed to cover “the Loss of the Insured arising from a Claim … for any actual or alleged Wrongful Act of any Insured in the rendering or failure to render Professional Services.” “Professional Services” were defined in the policy as “Those services of the Company permitted by law or regulation rendered by an Insured … pursuant to an agreement with the customer or client as long as such service is rendered for or on behalf of a customer or client of the Company:

(i) in return for a fee, commission or other compensation … or (ii) without Compensation as long as such non-compensated services are rendered in conjunction with services rendered for Compensation.'"

After a court ruled that the settlement costs didn't need to be paid by the insurer because the circumstances of the case didn't involve professional services, AISLIC filed suit in an attempt to recoup the money it had already advanced to PMI for defense fees and other legal expenses.

From PMI's point of view, it was at least entitled to the defense benefits. After all, the original suit had centered on an alleged violation of the Real Estate Settlement Procedures Act, a law that applies to professionals in the real estate and mortgage industries. So if the company was being accused of violating a law aimed at professionals, wouldn't that mean that the suit had indeed involved professional services?

A lower court didn't think so and said the suit revolved around administrative tasks, but the United States Court of Appeals for the Ninth Circuit felt otherwise. In its opinion, the court said the alleged kickbacks involved clients and professional insurance services and were therefore covered under the AISLIC policy.

Who is Covered Under an Errors and Omissions or Malpractice Policy?

In addition to taking different stances on what services and acts should be covered by their various professional liability policies, insurance companies often have their own views as to exactly who should be covered by their products. A doctor's malpractice insurance might provide some liability protection for nurses who are under the doctor's supervision or might leave a nurse entirely unprotected.

If a non-professional, such as a clerical worker, commits an error or omission that causes major economic damages for clients, that person might or might not be covered by a company's professional liability insurance policy. Consultants at law firms, insurance companies or engineering companies might be insured by a company policy, or they might need to shop for professional liability insurance on their own.

Package Deals

Besides the basic coverage available through errors and omissions insurance and malpractice insurance, many professionals who run their own businesses believe it's in their best interest to purchase other kinds of liability policies, too.

At least two products — employment practices liability insurance and fiduciary liability insurance — could probably be the focus of a separate insurance course, but they deserve, at least, their own paragraphs in this material because they are often marketed as part of comprehensive insurance products that combine some of the liability insurance features we have already addressed.

Employment Practices Liability Insurance

Employment practices liability insurance pays defense costs, settlements and damages when companies, directors, officers or lower-ranking employees are accused by current, former or prospective employees of violating their rights.

There are several situations that could lead to an employment practices liability claim, such as retaliation (in which an employee complains about an aspect of the workplace and is unfairly punished for speaking up), company monitoring of employees' computer use, sexual harassment and the innumerable chances for discrimination in the hiring, firing and promoting of workers.

Policy features, exclusions and premiums may depend on the number of employee-friendly laws in a buyer's state and on the risks presented by a particular business.

As in any other line of insurance, carriers offering EPL products will evaluate each applicant carefully by asking questions about the buyer's past, present and future susceptibility to risk. Here are some questions that might be particularly important to an underwriter when evaluating EPL risks:

- Have you ever been accused of an illegal employment practice, and if so, what was the outcome?
- How many people do you employ?
- How often do you experience employee turnover?
- What level of hiring, firing or layoffs have occurred recently or are likely to occur in the near future?

- Do you have a company policy manual that promotes consistent professional conduct at the workplace?
- Do you have a team of employees working exclusively in human resources? If so, how much influence does the team have in company decisions?
- In which states does your business operate? (This can be a factor because employment laws differ by state.)
- What types of information do you request on employment applications?
- What type of (and how much) training do you provide to employees on an initial and ongoing basis?

Coverage under an employment practices liability policy may be contingent on employees completing a training program that educates them about workplace issues.

Fiduciary Liability Insurance

Under the Employee Retirement Income Security Act of 1974 (ERISA), benefit plan administrators can be held personally liable for their mistakes. In addition to other plan concerns, company officials risk being sued by current employees, former employees and families if they make investment decisions that have a negative impact on benefits. They also could face trouble if the fees employees must pay in order to be covered by a plan are not considered reasonable.

Fiduciary liability insurance can be bought to guard against these risks. Like the other policies we have addressed in this chapter, fiduciary liability insurance can cover defense costs, settlements and damages. Insured parties may include a company, its directors and officers and past, present and future plan administrators.

Fiduciary liability insurance is sometimes packaged with "employee benefit liability insurance," which addresses similar risks but doesn't cover ERISA claims. An employee benefit liability policy might cover claims in which a plan administrator either made errors that prevented an employee from joining a plan or gave employees the wrong impression of what benefits were available through a plan.

Deductibles and Co-Payments

A professional liability policy—be it an errors and omissions contract or a malpractice contract—will probably cover valid claims for one year before needing to be renewed by mutual consent of the policyholder and the carrier. But, as is the case with many other insurance products, the fact that a claim is valid under the policy language hardly exempts the policyholder from having to pay any portion of that claim.

Insureds should expect to pay deductibles and co-payments, which let the insurance company take some of the financial risk off its own shoulders and give it back to policyholders. The "deductible" is the amount, expressed in dollars, which policyholders must pay on their own before an insurance company applies policy benefits to a claim. No matter the type of professional liability policy, the deductible is unlikely to be small. Deductibles for errors and omissions and malpractice policies can be sometimes be several thousand dollars.

Producers can negotiate with carriers in order to arrive at a deductible that reflects the buyer's risk tolerance and financial resources. In exchange for a lower deductible, the buyer will usually pay higher premiums. In exchange for lower premiums, the buyer will have to take on more risk by agreeing to a higher deductible.

The deductible in a professional liability policy can be applied in a number of different ways. A policy might call for a one-time aggregate deductible of $1,000, for example, while another policy might call for a $1,000 deductible on each claim filed during the policy's term.

A per-claim deductible, which tends to shelter the insurer from numerous small claims, doesn't need to be entirely inflexible. Related claims can be grouped together for the sake of the deductible. It's even possible to combine claims from a civil suit and claims from a criminal proceeding if all claims stemmed from the same error, omission or negligent act.

A professional liability policy might make exceptions for certain claims and require the policy's owner to pay no deductible at all in those cases. For instance, some but not all policies impose a deductible upon

settlements and damages, while applying consumer-friendly, first-dollar coverage to defense costs. This approach protects insureds from having to lose money as the result of frivolous lawsuits.

In addition to a deductible, professional liability policies might list a “co-insurance requirement,” which requires the insured to pay a portion of all claims even after a deductible has been satisfied. For example, a policy might require an insurer to pay 95 percent of each claim after a deductible has been met and require the insured to pay the remaining 5 percent.

Benefit Limits

When big or frequent liability claims arise, it will be important for insureds to know how close they are to reaching their benefit limit. A policy might have a “per-claim benefit limit” that caps coverage on each claim or an “aggregate benefit limit” that suspends coverage when total claims during a coverage period reach a certain dollar amount. A policy may have both a per-claim benefit limit and an aggregate benefit limit.

Like a deductible, a benefit limit might not apply to all kinds of claims. Buyers who are worried that expensive defense costs might erode their coverage and leave them with few benefits for settlements can shop around for a professional liability policy that excludes defense costs from benefit limits.

A wide range of benefit limits are common in the professional liability market. Sales professionals report that an insurance agent can have anywhere from $500,000 to several million dollars in errors and omissions coverage.

Towers of Coverage

In actuality, companies or professionals can probably snare as much liability insurance as they feel is necessary. To get it, they just need to be prepared to work with multiple insurers.

Many professionals buy policies from multiple carriers and construct high “towers” of coverage. At the base of a tower is the primary insurance policy, which is likely to be affected whenever an insured files a claim. Supplemental policies are stacked on top of the primary insurance policy and are put to work when benefits under the primary policy have been exhausted. When benefits under the primary policy and a supplemental policy have reached their limits, coverage under the next policy in a tower can kick in.

Insurance brokers are deeply involved in assembling towers of coverage for companies and are often responsible for ensuring that the multiple policies from multiple insurers fit together without leaving coverage gaps.

At first, layering policy upon policy might seem like an expensive approach to risk management. Though this financial assessment is probably true in many cases, buyers should remember that, at some point in a tower, higher levels of coverage start to become considerably less expensive. This eventual drop or leveling in price occurs when the probable size of a claim is highly unlikely to affect the upper portion of an insured’s tower.

Liability Premiums

Whether a person or company is planning to buy a new professional liability insurance policy or is hoping to renew an existing contract, price is certain to be a concern. Like all other kinds of insurance, professional liability coverage is priced based on the various risks that an insured party presents to an insurance company. When underwriting a candidate for professional liability insurance, a carrier must take into account not only the probable frequency of claims but also the probable size of those claims.

For obvious reasons, an applicant’s claims history and legal history will have a significant effect on the way a carrier views the applicant’s risk potential. A history of claims from an old policy could jeopardize the applicant’s chances of getting a new policy at a desired price, and claims on an existing policy could lead to trouble at renewal time. Claims or no claims, the insurer will probably be interested to know if the applicant has been sued and, if so, under what circumstances.

A spotless history, however, is sometimes not all an applicant needs to receive preferred premiums and benefits. After all, a law-abiding, ethically upright professional can sometimes be named in a suit, and shady people can get lucky and avoid having to go to court for years on end. To minimize the luck factor, an insurer

may ask new or renewing customers about the safeguards they have put in place to keep claims at a minimum.

The professional's experience level can also have an effect on premiums. Like a newly licensed driver applying for auto insurance, freshly licensed insurance producers might need to wait a few years before they become eligible for less expensive errors and omissions coverage.

The price for policies will often depend on the specifics of the services that are provided by the insured. Premiums for legal malpractice coverage may depend on the area of law that an attorney practices. Likewise, doctors in one line of medicine will pay different rates than physicians with other specialties.

If an individual has a specialty within a profession, the insurer might base part of a premium on how often the person ventures outside of that specialty to perform other services. For example, an engineer who focuses strictly on environmental engineering might be able to get a better rate than someone who works as a structural engineer and as an environmental engineer.

Claims-Made Policies and Occurrence Policies

Based on the way they handle claims, liability insurance contracts can be deemed either "claims-made policies" or "occurrence policies."

Claims-made policies cover claims that arise during the applicable coverage period. If damage is done during the coverage period but a person waits until after the coverage period to make a claim, the insurance company can deny the claim.

On the other hand, a claim on an occurrence policy can be made at any time, as long as the damage that provoked the claim was done during the coverage period.

As an example, think of a doctor who performed surgery on a patient in 2006 and was sued yesterday for performing the surgery in a negligent manner. Then pretend that the doctor had left the medical profession at the end of 2006 and did not renew his malpractice insurance. If the doctor's insurance was written on a claims-made basis, he might not be covered at all and need to pay out of pocket to defend himself. However, he might still have coverage if his insurance was written on an occurrence basis, since coverage under an occurrence policy depends on when the alleged wrongdoing took place and does not depend on the timing of a claim.

Pros and Cons of Occurrence Policies

Some experts in their fields advise their fellow professionals to buy an occurrence policy if one is made available to them. The coverage is broader than claims-made coverage and puts less pressure on insureds to report claims quickly. But occurrence policies have their drawbacks.

The reduction in time sensitivity can give insureds a false sense of security and make them think that their coverage for past errors lasts forever. In reality, each occurrence policy—like any other kind of insurance—only provides benefits up to a certain dollar amount. If previous claims have exhausted policy benefits, an otherwise valid claim can still be denied by the insurance company.

Occurrence policies also tend to be more expensive than claims-made policies because the policies' benefits can last longer. With an occurrence policy, an insurance company is obligated to pay claims after cancellation and therefore absorbs risks for a longer period of time. Conversely, insurers can charge less for a claims-made policy because they do not need to honor claims after a cancellation, unless the policyholder opts for extended coverage and pays an additional fee.

Particularly in regard to professional liability, determining coverage under an occurrence policy can be challenging for an insurer. While other kinds of insurance claims (such as property claims under fire or auto policies) can be easily traced to a specific event that occurred on a specific date, insurers may struggle to determine exactly when an error, omission or an instance of professional negligence took place. Because an insurer can't count on an insured person to always document errors in judgment as they occur, insurance companies may find it easier to offer professional liability insurance through claims-made policies.

Media Liability Insurance

For various reasons, occurrence policies for professional liability insurance are far less common today than they were in years past. In fact, “media liability insurance” may be one of the few kinds of professional liability coverage that a modern-day insurer will provide customarily on an occurrence basis. This insurance, which protects insureds against claims involving libel and slander, is different compared to the other kinds of coverage we have addressed thus far, in that a media liability claim can almost always be traced back to a specific event that occurred on a specific date. Libel can be traced back to the date when the allegedly libelous comments were published, and slander can be traced back to the date when the allegedly slanderous comments were spoken to the public.

Reporting Liability Claims

Most errors and omissions and malpractice insurance contracts are claims-made policies. These polices can make the timely reporting of claims more important than many insureds realize. In fact, it’s not uncommon for an otherwise valid claim to be denied by an insurer all because a policyholder did not report the situation promptly to the carrier.

For clarity purposes, “reporting” a potential or real claim may be defined as communicating with the insurer about the claim in a reasonable way. It’s advisable and sometimes necessary for insureds to report not only an actual demand for money but also any situations that are likely to result in a demand for money as soon as possible. The requirement to report potential claims is sometimes known as a “notice of circumstance.” Depending on the policy, an insured might need to provide notice of circumstance within 60 to 90 days of knowing about a potential claim.

Still, an insurer’s strict attitude toward the reporting of claims can occasionally work in the consumer’s favor. Among the claims-made policies that require insureds to give notice of potential claims, a few make it possible for policyholders to report potential claims, cancel their coverage and still be covered for defense and settlement costs if a real claim arises at a later date.

Prior Acts

Like all kinds of claims-made policies, liability insurance for professionals can have major gaps near the beginning and the end of coverage periods. Most of these policies contain some kind of “prior acts exclusion,” which excuses the insurer from having to cover claims when an insured’s error, omission or negligent behavior occurred before the liability insurance took effect.

Suppose an uninsured insurance agent works with clients and performs his duties negligently. Then, before the affected clients become aware of the negligence, the agent buys an errors and omissions policy for himself. Two months later, a client realizes she has been wronged and files suit against the agent. The opposing parties work out a settlement, and claims are then filed with the agent’s insurance company. Although the claims are made within the coverage period, the insurer is able to deny the claim because the negligence leading up to the claim occurred before the agent bought his policy.

Nose Coverage

Many insurance companies offer “nose coverage,” which protects insureds when a claim occurs during a coverage period but the error, omission or negligence occurred before the coverage period. In other words, nose coverage can handle claims that would otherwise be denied on the basis of a prior acts exclusion.

Nose coverage is often bought when a professional switches from a claims-made policy to an occurrence policy, but it can also be bought by people who are replacing one claims-made policy with another and by people who have never had any form of professional liability insurance. However, nose coverage is usually not necessary if someone is replacing an occurrence policy, since prior acts excluded by a new claims-made or occurrence policy are likely to be covered under a lapsed or cancelled occurrence policy.

The extent of an insured’s nose coverage depends on a “retroactive date.” When a claim arises and the related act was committed on or after the retroactive date, the nose coverage kicks in and protects the insured. When a claim arises and the related act was committed before the retroactive date, the insured is not protected by the nose coverage.

If the buyer purchases nose coverage from the start, the policy's retroactive date will typically not change when the person renews the policy. If the buyer doesn't purchase nose coverage from the start, renewed policies will have a retroactive date that reaches as far back as the day coverage originally began.

So, in spite of the typical one-year coverage period for most professional liability policies, someone who bought a policy on Jan. 1, 2018, will continue to be covered for acts committed on and after that date in subsequent years, as long as the policyholder pays premiums on time and renews the insurance consistently.

When companies or individuals purchase a new claims-made liability policy instead of renewing an old one, they can arrange for nose coverage to retroactively date back to the first day of coverage under the old policy. If an applicant has never had a professional liability policy, the insurer can arrange for nose coverage that dates back to the day a company or individual first started providing professional services.

Tail Coverage

"Tail coverage" can be an alternative to nose coverage if a professional is replacing a claims-made policy or has no intention of renewing or replacing a claims-made policy. Tail coverage gives insureds an "extended reporting period," which allows people to report professional liability claims and have them covered even if coverage has otherwise been cancelled or has expired. This coverage doesn't apply to errors, omissions or negligent acts that occur after a policy has been cancelled, but it does protect former policyholders when an act that was committed during the policy period creates legal problems in the present.

Perhaps the easiest way to understand how tail coverage works is to think of a retired professional. Pretend an attorney retired at the end of 2017 and chose not to renew her malpractice insurance. This year, a former client sued the attorney for negligence, claiming that she had an improper and damaging effect on a court case. Although the attorney cancelled her insurance coverage in 2017, her defense costs and other legal expenses might still be paid for by her old insurer if she had purchased tail coverage.

Insurers are often required to offer tail coverage to insureds when liability insurance is cancelled or not renewed. Exceptions to this requirement might include cases in which a policyholder hasn't paid premiums or has misrepresented facts to the insurance company. Research conducted for this course showed that tail coverage often lasts within the range of three to six years, though coverage of one year is not unheard of and coverage over an insured's lifetime may be possible. In some cases, tail coverage might even be included for no additional charge if the incident relating to a claim is reported to the insurance company within a month or two of cancellation.

Additional premiums for tail coverage are typically based on the price of liability insurance during the old policy's final year. The lawyer in the preceding example, for instance, would have probably paid a tail premium equal to her 2017 annual premium, multiplied by 100 percent, 150 percent or some higher percentage. An insurer may provide discounted tail coverage to professionals who are canceling their policies due to retirement or disability.

It should be noted that many people use the terms "tail coverage," "extended reporting period" and "discovery period" interchangeably, while others use these phrases to mean slightly different things. To some producers, a "discovery period" is a short-term extended reporting period that is included within a professional liability policy at little or no charge. These producers may reserve the term "tail coverage" for longer and pricier extended reporting periods that the insurer sometimes offers to clients at its own discretion.

Defense Costs

Even careful and ethical professionals may have to defend themselves against charges of negligence, malpractice or some other alleged misdeed, and even a suit that leads to a dismissal or a "not guilty" verdict can be an extremely expensive distraction for the accused. On its own, the cost of defending oneself against bogus charges can equal thousands of dollars, or perhaps even more if a person employs top-notch representation in a drawn-out court case. With the price of pleading their innocence often running so high, many companies and individuals place as much importance on a policy's ability to absorb defense costs as they do on its ability to cover settlements and court-awarded damages.

Almost all errors and omissions policies and malpractice policies force an insurer to pay defense costs when a suit involves an act or risk that is covered under the insurance contract. Once it begins paying these costs, the insurer generally cannot suspend payments unless it can conclusively show that the suit doesn't involve a covered act or can conclusively show that it is within its rights to cancel coverage.

Though insured persons can take comfort in knowing that their policy will help them pay for legal fees under several circumstances, they shouldn't ignore the limitations and particulars of their contract's defense provisions. Unlike many forms of general liability insurance, the kinds of insurance we have focused on in these pages usually apply defense costs to policy limits. In other words, if an insurance agent is covered by a $500,000 errors and omissions policy and his insurer pays out $500,000 for defense costs, there might not be any money left over to cover settlements, court-awarded damages or any other claims. It's also important to remember that an insured may need to pay for some defense costs out of pocket until a policy's deductible has been satisfied.

Duty to Defend

When a suit is filed against an insured, the professional's relationship with a carrier will depend on whether the policy puts a "duty to defend" upon the insurance company's shoulders. When a policy creates a duty to defend, the insurance company is responsible for contesting claims with plaintiffs. This responsibility can give the insurer immense control over the defense process. In cases in which a duty to defend exists, the insurer can choose the defense team that will be entrusted with handling the suit, or it can pre-approve a list of legal professionals and require the insured to choose defense counsel from that list. A duty to defend can also give an insurer the power to approve defense strategies.

Some liability policies for professionals and high-ranking corporate officials don't create a duty to defend. However, the absence of a duty to defend doesn't allow an insurer to avoid paying defense costs, and it doesn't completely eliminate an insurer's power over the defense process.

A professional liability insurer without a duty to defend often can't force legal counsel upon a defendant, but it may still have the right to veto the insured's choice for representation. After a defense team has been put in place, the insurer can refuse to pay attorneys' fees if the services being provided by the defense team or the costs of those services aren't considered reasonable. From a procedural standpoint, an insurer without a duty to defend may still require that an insured's lawyers work on an hourly basis and keep an accurate record of the time they spend performing various tasks. Regardless of a policy's aggregate benefit limit, the insurance contract can impose a per-hour cap on reimbursable attorneys' fees.

Even without a duty to defend, the insurer often must be kept in the loop throughout the stages of a case so that it can evaluate the size of potential claims and get an idea of when a court decision or settlement might be forthcoming.

Timing of Defense Benefits

Due to the huge expenses involved with defending oneself in a lawsuit, it will be important for professional liability policyholders to know when they can expect to receive reimbursements for defense costs. Policy benefits that cover defense costs can either be advanced to defendants when a lawsuit is filed, or they can be paid to insureds at a later date after legal services have already been rendered.

Nearly every insurance customer would probably prefer to receive money for defense costs as an advance, since this kind of arrangement puts less economic stress on the insured and can give an innocent professional more courage to refute a plaintiff's charges. If defendants need to bankroll their own defense before benefits arrive, they may worry about not having enough personal assets to pay for their immediate expenses and could end up accepting an unfavorable settlement out of desperation. If they can get an advance from their insurer for legal expenses, they may be more likely to hold out for a fairer settlement or seek an appeal of a court's unfavorable ruling.

Many insurers will advance some defense money to their customers, perhaps operating under the assumption that people are innocent until proven guilty. But some guilty verdicts, such as those pertaining to fraud, can lead an insurer to rescind its generosity and require the insured to return the advanced funds.

Reservation of Rights

The possibility that an insurer may demand repayment of defense costs is often articulated in a “reservation of rights letter,” which is sent to an insured by the carrier if the validity of a claim is uncertain. Through this notice, the insurer informs the insured that it will give the person the benefit of the doubt and cover defense costs related to a questionable claim. Yet if the company later determines that the claim should not be covered under the policy for any reason, the reservation of rights allows the insurer to stop paying defense costs, deny coverage of any eventual settlement or court-awarded damages and possibly recoup insurance money from the insured.

Settlements

With all the exciting courtroom drama that can be found on television shows, movies and popular fiction, it can be easy for people outside the legal profession to forget that a huge number of lawsuits don’t go on long enough to merit a final verdict from a jury or judge.

Defendants may have several reasons to prefer a settlement over continued court proceedings, and many of those reasons have little to do with the accused actually being at fault. For one, the judicial process can be very tedious, with people on both sides of a suit often waiting several years for a final verdict. As more and more money, energy, worry and patience is invested in a case, defendants might believe it is in their best economic, physical and emotional interests to put an end to all the legal fighting and get on with their lives.

Sometimes, too, innocent defendants check their emotions at the door, take a step back from their situations and recognize that, for whatever reason, a judgment in their favor is highly unlikely. Perhaps a professional’s defense is too packed with jargon and technical know-how for a jury of laypersons to sympathize with. A medical malpractice case, for example, might hinge on a complex anatomical issue, while a corporate director’s defense in a liability case might be linked to a dry and complicated securities law.

Or maybe the professional is tempted to settle a suit because a court’s harsh verdict could put the person’s financial health in serious danger. When a court is likely to award damages to a plaintiff that are in excess of a defendant’s insurance benefits, the defendant’s legal team will probably level with its client and recommend settling the suit.

Though liability insurers and their policyholders can benefit from settling certain claims, a carrier and an insured may become annoyed with each other when one of them wants to settle a case and the other wants to fight it. Luckily for each of them, many professional liability insurers recognize the potential for tension and address this issue in their policies so that both sides may understand their rights.

If a professional wants to settle a suit against an insurer’s wishes, the insurer generally can’t prevent a settlement from taking place. It makes no difference if the insurer suspects that the professional committed fraud or some other wrongful act and is hoping to use a court’s final ruling as grounds for denying a claim or rescinding coverage altogether. Policyholders just need to give notice to their insurer when they are prepared to settle with plaintiffs. Similar notification will be necessary if an insured intends to admit guilt in a case in the hope of receiving a lighter sentence.

Often, the insurer is the one that wants to settle, and the insured is the one who wants to prolong a legal dispute. When this occurs, many liability policies purchased from non-admitted carriers put the policyholder at the mercy of the insurer and let the carrier settle a case on its own. Other policies feature a “consent to settle clause” and require that the insured approve a proposed settlement before it can be executed.

A consent to settle clause might only let the insured give a “yes” or “no” response to a proposed settlement, while leaving the person in the dark about the size and particulars of the deal. In most forms, a consent to settle clause is only relevant if an insured’s refusal to settle is reasonable. Otherwise, an insurance company may be able to settle with a plaintiff without the person’s approval.

Hammer Clauses

Other pieces of a professional liability policy respect an insurer’s desire to settle claims but allow policyholders to continue fighting a lawsuit if they so choose.

When an insured doesn't consent to a proposed settlement, the insurance company can invoke a policy's "hammer clause." A hammer clause basically states that the insurer will cover a liability claim equal to the amount of a proposed settlement and will deny any liability claim that is in excess of that amount.

Suppose an attorney was sued for malpractice and that the plaintiff was originally willing to settle the case for $500,000. The attorney did not agree to the deal, and his insurer invoked his policy's hammer clause. If the attorney ends up losing his case and is required to pay the plaintiff $500,000 or less, he may be able to have his claim covered nearly in full by his insurer. However, if he loses and must pay $1 million to the plaintiff, he will need to pay at least $500,000 out of his own pocket.

Some hammer clauses only make the insured responsible for paying excessive damages and excessive settlements, while keeping coverage of defense costs intact. Others can introduce limits on defense benefits.

It's also possible for a policy to contain a "soft hammer clause," which splits the responsibility for paying excessive claims between the insurer and the professional. By invoking a soft hammer clause, the insurer might agree to pay claims equal to a proposed settlement and cover 50 percent of claims above that amount.

A few policies contain "carrot clauses," which don't penalize professionals for turning down a settlement but give them a positive incentive to accept one. For instance, under a carrot clause, professionals might be able to reduce their deductible if they agree to settle a suit early.

Policy Exclusions

As helpful as errors and omissions policies and malpractice policies can be for professionals, they do tend to contain many exclusions.

It is best for an insured to understand these exclusions before a claim arises. When an insurance professional discloses and explains policy exclusions to a buyer early in their relationship, the consumer has more time to fill in coverage gaps, and the potential for coverage disputes is reduced.

The next few pages highlight many of the exclusions that apply to various liability policies. Though readers should note that many of the mentioned exclusions are reserved for specific groups of professionals, there is also some occasional overlap.

Coverage Under Other Polices

All the professional liability policies discussed in this text tend to exclude coverage of perils and events that can be covered by another kind of insurance policy. Claims for property damage and bodily injury may be covered by a company's general liability insurance, so a professional liability policy is unlikely to pay such claims. Product liability insurance is its own product and is also excluded from professional liability contracts. The same is true for insurance that protects companies and individuals who are accused of slander or libel. It may be possible for a company to purchase all these other kinds of insurance from the same carrier as part of a package that also includes professional liability coverage.

Insured vs. Insured Exclusion

In an effort to prevent policyholders from using their insurance coverage as an instrument of fraud, many liability contracts contain an "insured vs. insured exclusion." This exclusion lets the insurance company deny claims when the opposing parties in a lawsuit are covered by the same policy. This exclusion is most commonly an issue for corporate directors and officers (who will not have coverage if they are sued by their own companies), but it occasionally applies to non-corporate professionals, too. A medical malpractice policy that covers a doctor and his nurse, for instance, might not provide benefits to the doctor if he performs a medical procedure on the nurse and is sued for negligence.

Pollution Exclusions

Several liability policies specifically exclude coverage for pollution claims. This exclusion can create a big insurance gap for design professionals who may have worked with lead-based paint or are linked to an asbestos problem. Corporate executives are also affected by this exclusion when their companies produce products that harm the environment or perform services that create pollution.

In many cases, this gap can be eliminated through the purchase of an "environmental insurance policy," which can cover the cost of cleanups and the consequences of hazardous spills.

Pollution Claims

Cultural changes and current events make insurers' use of pollution exclusions something to keep an eye on. Scientists, politicians, news outlets and the general public have heaped tremendous amounts of attention on the issue of global warming in recent years, and it may be just a matter of time before many companies are pulled into court due to their alleged roles in climate change. Yet even within the large faction that does not doubt climate change is a real problem, there is a debate as to whether greenhouse gas (a main culprit in climate change) is technically a pollutant in the traditional sense of the word.

With that in mind, it will be interesting to see how liability insurers respond. Will they be able to deny global warming claims through their preexisting pollution exclusions, or will they add specific language to the policies in order to protect themselves?

At this point, one may even predict that the industry will respond to global warming in much of the same way that some insurers responded to terrorism in 21st century: by working around policy exclusions and creating a product that meets clients' modern needs.

Other Exclusions

Other exclusions have received less attention from the people who sell insurance and the people who write about the industry. Admittedly, some of the lesser-known exclusions are only applicable to specific kinds of clients. However, since producers are likely to encounter a broad variety of professionals in need of liability protection, it is important for them to at least be aware that these various exclusions exist.

An errors and omissions policy or malpractice policy may or may not cover the following:

- Punitive damages.
- Taxes.
- Privacy breaches.
- Discrimination claims.
- Cases in which a company is sued for not having bought adequate insurance.
- Cases in which an insurance producer inappropriately gave clients tax advice.
- Cases in which an insurance producer participated in bid-rigging, rebating or wet-ink transactions.
- Cases in which insurance producers failed to disclose the duties they owe or don't owe to clients as agents or brokers.
- Cases in which directors and officers are accused of violating the Employee Retirement Income Security Act.
- Cases in which medical professionals gave free advice or provided free services and are accused of malpractice.

Policy Rescissions and Severability

In addition to having the right to deny a specific claim, a liability insurer reserves the right to "rescind," or revoke, an entire liability policy under certain circumstances. In a rescission, coverage not only ends earlier than expected but is treated as if it never existed. The insurer and the insured essentially act as if they never entered into a contractual relationship in the first place.

Grounds for rescission are few, making this total cancellation of coverage relatively rare. An insurance company may rescind a professional liability policy when the policyholder fails to pay the required premiums on time or when it is determined that the filled-out application for the insurance contained untruths.

The insurer's ability to cancel coverage in these situations probably seems reasonable enough to most people. Insurance companies don't want to give coverage away for nothing, and they do not want to be misled about the nature of the risks that they undertake.

Still, the insurer's right to rescission is not as clean-cut as it may seem, particularly when it comes to untrue statements on an insurance application. When an insurance company wishes to rescind a policy due to an applicant's misrepresentations, the burden of proof is on the insurance company. In other words, the applicant is considered innocent until proven guilty and remains covered until the insurer can conclusively show that misrepresentations occurred.

An insurer may not be able to rescind a policy, regardless of a misrepresentation, if the insurer should have reasonably known about the misrepresentation when it was made or if the misrepresentation did not influence the way the insurer offered coverage to the applicant. When an insurer is successful in rescinding a policy, it typically must give affected policyholders a refund of their premiums.

Conclusion

Considering all the liability risks that exist for professionals, a nervous observer may wonder why anyone would dare become a doctor, lawyer or insurance agent or other specialist with significant responsibilities.

Apprehensive men and women who long for a professional career but shy away from one for fear of a legal dispute should realize that competence and care are not a person's only shield in battles against liability. With the help of a knowledgeable insurance producer, they may be able to obtain a liability insurance policy that offers the necessary protection.

BOOKMARKEDUCATION

CALIFORNIA INSURANCE CE

Satisfy your entire CE requirement.
Discount packages are available.

Choose a package
and SAVE!

Don't Delay, Enroll Today

Online:

BookmarkEducation.com

Phone:

(800) 716-4113