Health Law Developments

The Newsletter of the Health Law Section
State Bar of Georgia
Winter 2018

Inside This Issue

From the Chair

Dear Friends and Colleagues,

Happy New Year! We are excited about the year ahead and grateful to our outgoing Chairperson, Keith Mauriello, for his long and continuing service to our Section. Thank you, Keith.

As the new Chairperson of the Health Law Section, I look forward to working with Keith and our wonderful Section Officers and Executive Committee to bring you another year of meaningful programs and networking opportunities.

We encourage you to contact us to learn more about our upcoming events and to get involved:

- Law School Outreach – connect with Georgia law students studying health law
- Mentor Program – help us launch a mentor program for new health law lawyers
- Lunchtime CLE – suggest a good topic, organize a panel, or attend a lunch program
- Nonprofit Night – participate in a fundraiser dinner for a local healthcare nonprofit
- Newsletter – write an article for our Spring newsletter

This is just a start. We have many more exciting events on the horizon. We are also exploring ways to expand our services for Section members who live outside of the Atlanta region. We welcome your suggestions.

Best regards,

Lynn M. Adam, Chairperson, Health Law Section

From Epidemic to Crackdown: The Government's Fight Against Opioid Fraud and Abuse

by Scott R. Grubman[1]

Introduction

Since taking the helm of the Department of Justice (DOJ), Attorney General Jeff Sessions has made clear that the federal government will continue its enforcement efforts within the healthcare industry. At the forefront of those efforts is increased enforcement related to opioid prescribing and abuse. The first major public action by the DOJ related to opioid fraud and abuse enforcement came in July 2017, when it announced the largest healthcare fraud takedown in history. Out of the 412 defendants charged as a part of that takedown, over 120 were charged for their roles in prescribing and distributing opioids and other dangerous narcotics. A few weeks later, on August 2, 2017, Attorney General Sessions announced the formation of the DOJ's Opioid Fraud and Abuse Detection Unit. According to the DOJ's press release, the pilot program will "utilize data to help combat the devastating opioid crisis that is ravaging communities across America." This article will explore the history of those efforts, and discuss the DOJ's new pilot program, as well as efforts by states to combat opioid fraud and abuse.

Brief Overview of the Opioid Epidemic

According to the Department of Health and Human Services (HHS), opioid abuse is a "serious public health issue," with drug overdose deaths representing the leading cause of injury death in the United States. The National Institute on Drug Abuse — part of the National Institutes of Health (NIH) — notes that young adults age 18 to 25 are the biggest abusers of prescription opioid pain relievers, attention deficit hyperactivity disorder (ADHD) stimulants, and anti-anxiety drugs. NIH reports that in 2014 alone, more than 1,700 young adults died from prescription drug overdoses, and most of those overdoses involved opioids. The Centers for Disease Control and Prevention (CDC) reports that over 90 Americans die every day from an opioid overdose. According to the CDC, more than 60 percent of drug overdose deaths involve an opioid and, since 1999, the number of overdose deaths involving opioids quadrupled.

The Feds Fight Back

The federal response to the opioid epidemic has continued to intensify over the last several years. Perhaps not surprisingly, the Food and Drug Administration (FDA) was on the forefront of the fight against opioid addiction. In 2013, for example, the FDA issued draft industry guidance entitled "Abuse-Deterrent Opioids – Evaluating and Labeling." That guidance was "intended to assist sponsors who wish to develop opioid drug products with potentially abuse-deterrent properties." That industry guidance was finalized in April 2015. Similarly, in March 2016, the FDA released draft guidance entitled "General Principles for Evaluating the Abuse Deterrence of Generic Solid Oral Opioid Drug Products," and in May 2017 issued draft guidance entitled "FDA Education Blueprint for Health Care Providers Involved in the Management or Support of Patients with Pain."

The FDA has also developed a comprehensive action plan to fight the opioid epidemic. The FDA's Opioids Action Plan includes: (1) expanding the use of expert advisory committees before approving any new drug application for an opioid that does not have abuse-deterrent properties; (2) developing warnings and safety information for immediate-release (IR) opioid labeling; (3) strengthening requirements that drug companies generate post-market data on the long-term impact of using opioids; (4) updating the Risk Evaluation and Mitigation Strategy (REMS) Program, which requires sponsors to fund continuing medical education related to opioid issues; (5) expanding access to abuse-deterrent formulations to discourage abuse; (6) supporting better treatment by healthcare providers; and (7) reassessing the risk-benefit approval framework for opioid use.

Like the FDA, the federal Office of the National Coordinator for Health Information Technology (ONC) has also taken steps to combat opioid abuse. According to ONC guidance, one of the leading tools to combat opioid abuse is electronic prescribing. ONC states that:

Electronic prescribing of controlled substances (EPCS), legal in all 50 states, helps reduce fraud and abuse of controlled substances like prescription opioids. Moving from paper-based prescribing to EPCS enables providers to make use of enhanced security features that technology affords. Prescribers can be authenticated before prescribing a controlled substance and prescriptions may be transmitted to pharmacies securely without the risk of alteration or diversion.

As of Sept. 30, 2016 (which is the latest data available), over 88 percent of retail pharmacies and over 20 percent of e-prescribing providers were enabled for EPCS.

Another important IT tool in the government's fight against the opioid epidemic are prescription drug monitoring programs (PDMPs), which are state-run databases that provide information to healthcare providers related to a patient's history of controlled substance

prescription use. According to ONC, PDMPs "are one of the most promising tools available to address prescription drug misuse, abuse, and diversion." ONC promotes the use of PDMPs to "avoid inappropriate prescribing, identify drug-seeking behavior, and allow[] providers to intervene when there are signs of prescription drug misuse."

HHS' Office of Inspector General (OIG) has also taken an increasingly aggressive approach to fighting the opioid crisis. In addition to its partnership with the DOJ (discussed in more detail below), the OIG has used its own law enforcement and administrative powers to detect and punish opioid fraud and abuse. For example, in July 2017, the OIG published a report entitled "Opioids in Medicare Part D: Concerns about Extreme Use and Questionable Prescribing." The "key takeaways" from the OIG's report include:

- One in three Medicare Part D beneficiaries received a prescription opioid in 2016;
- About 50,000 beneficiaries received high amounts of opioids;
- Almost 90,000 beneficiaries are at serious risk; some received extreme amounts of opioids, while others appeared to be doctor shopping;
- About 400 prescribers had questionable opioid prescribing patterns for beneficiaries at serious risk.
- In its report, the OIG noted that prescribers "play a key role in combatting opioid misuse" and that such prescribers "must be given the information and tools needed to appropriately prescribe opioids when medically necessary."

The DOJ Jumps In

Even before the DOJ's announcement regarding the Opioid Fraud and Abuse Detection Unit, the agency made clear that the fight against opioid fraud and abuse is a top priority under the new administration. As discussed above, for example, nearly one-third of the defendants charged in the DOJ's July 2017 healthcare fraud takedown were charged in schemes related to prescribing and dispensing opioid and other narcotic drugs:

The charges announced today aggressively target schemes billing Medicare, Medicaid, and TRICARE . . . for medically unnecessary prescription drugs and compounded medications that often were never even purchased and/or distributed to beneficiaries. The charges also involve individuals contributing to the opioid epidemic, with a particular focus on medical professionals involved in the unlawful distribution of opioids and other prescription narcotics, a particular focus for the Department.

The fact that the DOJ immediately followed up on this takedown by announcing the creation of the Opioid Fraud and Abuse Detection Unit demonstrates the agency's long-term focus on such cases. In announcing the new unit, Attorney General Sessions stated that it will "focus specifically on opioid-related health care fraud using data to identify and prosecute individuals that are contributing to this prescription opioid epidemic."

As part of the initiative, the DOJ will fund 12 experienced Assistant United States Attorneys from various offices around the country for a three-year term to focus exclusively on investigating and prosecuting fraud related to prescription opioids, including pill mills and pharmacies that unlawfully divert or dispense prescription opioids for unlawful purposes. The 12 districts that will participate in the pilot program are: the Middle District of Florida, Eastern District of Michigan, Northern District of Alabama, Eastern District of Tennessee, District of Nevada, Eastern District of Kentucky, District of Maryland, Western District of Pennsylvania, Southern District of Ohio, Eastern District of California, Middle District of North Carolina, and Southern District of West Virginia.

According to the DOJ's press release, data analysis will allow federal authorities to ascertain important information related to prescription opioids, including which physicians are outliers in the number of opioid prescriptions, how many of a prescriber's patients die due to an opioid overdose, and which pharmacies are dispensing disproportionately large amounts of opioids. The DOJ will work with several federal agencies — including the Federal Bureau of Investigation (FBI), Drug Enforcement Administration (DEA), and HHS — as well as state and local law enforcement on the project.

Likely Areas of Focus

There are several areas on which the government will likely focus in its opioid-related investigations. The first will likely be ensuring that providers prescribe opioids and other narcotics only when such drugs are truly medically necessary. One of the basic principles of Medicare reimbursement is that all items and services for which a provider seeks reimbursement must be "reasonable and necessary." Providers who stand out as "outliers" when it comes to the volume of opioid prescriptions will likely receive subpoenas for relevant medical records from the DOJ and, if those records do not support the medical necessity of those prescriptions, will likely face administrative, civil, or even perhaps criminal liability.

Another focus will likely be on the relationships between prescribing physicians, on the one hand, and pharmaceutical companies and pharmacies, on the other. Because any financial relationship between a prescribing provider and a pharmaceutical company or pharmacy could potentially implicate both the Anti-Kickback Statute and the Stark Law, federal investigators will almost certainly probe any such relationships, particularly where the provider in question has questionable prescribing patterns or high utilization numbers. Other likely areas of focus will be on pharmacies that dispense a high number of opioids from providers with questionable prescribing habits, as well as enforcement of drug diversion regulations by the DEA.

State Attorneys General Get Involved

One month after AG Sessions announced the formation

of the DOJ unit, a coalition of forty-one state attorneys general announced a joint investigation focusing on major pharmaceutical companies over the production and distribution of opioids. On Sept. 19, 2017, New York Attorney General Eric Schneiderman announced that the joint investigation was initiated by the service of subpoenas on five major pharmaceutical manufacturers: Endo International, Janssen Pharmaceuticals, Teva Pharmaceutical Industries/Cephalon, and Allergan. Subpoenas were also served on three large pharmaceutical distributors: AmerisourceBergen, Cardinal Health, and McKesson. This state coalition is hoping to better understand what role the pharmaceutical industry's marketing and distribution methods have played in the opioid epidemic, and to analyze whether the industry should have any responsibility to help pay for the damage caused by the epidemic.

Conclusion

The new administration has made clear that healthcare fraud and abuse enforcement will remain a top priority, and fraud and abuse enforcement related to the prescribing and dispensing of opioid drugs is now clearly front and center. Although the DOJ's Opioid Fraud and Abuse Detection Unit is being called a "pilot program" and is currently limited to 12 districts, like many initiatives within the area of healthcare fraud and abuse this unit will likely grow into other jurisdictions in the not-so-distant future. Moreover, the states have made clear that they will be joining the federal government in the fight against opioid fraud and abuse, with a particular focus on manufacturers and distributors. As a result, those involved in any way in the opioid industry, including pain management providers, pharmacies, pharmaceutical manufacturers and distributors, will likely feel the heat of increased government enforcement for years to come.

Endnotes

1. Scott Grubman is a partner at Chilivis Cochran Larkins & Bever LLP
2. https://www.justice.gov/opa/pr/national-health-care-fraud-takedown-results-charges-against-over-412-individuals-responsible.
3. Id.
4. See https://www.justice.gov/opa/pr/attorney-general-sessions-announces-opioid-fraud-and-abuse-detection-unit.
5. Id.
6. Portions of this article were previously published by the American Bar Association's Health eSource, and are being re-published here with express permission.
7. https://www.hhs.gov/opioids/about-the-epidemic/index.html.
8. https://www.drugabuse.gov/related-topics/trends-statistics/infographics/abuse-prescription-rx-drugs-affects-young-adults-most.
9. Id. 2014 data is the latest data that the author could find on this topic.
10. https://www.cdc.gov/drugoverdose/epidemic/index.html.
11. Id.
12. https://www.fda.gov/downloads/Drugs/GuidanceComplianceRegulatoryInformation/Guidances/UCM334743.pdf.
13. Id.
14. https://www.fda.gov/downloads/Drugs/GuidanceComplianceRegulatoryInformation/Guidances/UCM334743.pdf.
15. https://www.fda.gov/downloads/Drugs/GuidanceComplianceRegulatoryInformation/Guidances/UCM492172.pdf.
16. https://www.fda.gov/downloads/Drugs/NewsEvents/UCM557071.pdf.
17. https://www.fda.gov/NewsEvents/Newsroom/FactSheets/ucm484714.htm.
18. https://www.healthit.gov/opioids/epcs.
19. Id.
20. Id.
21. https://www.healthit.gov/PDMP.
22. Id.
23. https://oig.hhs.gov/oei/reports/oei-02-17-00250.pdf.
24. Id.
25. Id.
26. https://www.justice.gov/opa/pr/national-health-care-fraud-takedown-results-charges-against-over-412-individuals-responsible.
27. https://www.justice.gov/opa/pr/attorney-general-sessions-announces-opioid-fraud-and-abuse-detection-unit.
28. Id.
29. Id.
30. Social Security Act, § 1862, 42 U.S.C. § 1395y(a)(1)(A).
31. https://ag.ny.gov/press-release/ag-schneiderman-bipartisan-coalition-ags-expand-multistate-investigation-opioid-crisis.
32. Id.
33. Id.
34. http://www.npr.org/sections/thetwo-way/2017/09/19/552135830/41-states-to-investigate-pharmaceutical-companies-over-opioids.
35. For example, the DOJ-HHS Medicare Fraud Strike Force started in 2007 in four cities, and quickly expanded to a number of other cities within just a couple of years. See https://oig.hhs.gov/fraud/strike-force/.

Pro Bono Partnership of Atlanta provides pro bono opportunities specifically geared toward transactional lawyers, including healthcare attorneys. Attorneys provide advice in their area of expertise to 501c3 charities that serve low-income or disadvantaged individuals and cannot afford legal services. The current volunteer opportunities are available at http://www.pbpatl.org/for-attorneys/volunteer-opportunities/. If you are interested in volunteering or want to receive the monthly email with volunteer opportunities, please email Rachel Spears at rachel.spears@pbpatl.org.

Structuring Provider Transactions to Prevent Practice Pitfalls: Deeply Rooted Corporate Practice Doctrine Remains Strong

by Ernessa B. McKie[1]

With growing patient demands, advanced technology and payer restraints, healthcare providers are increasingly exploring management agreements with experienced companies to handle the daily operations of their clinical practice. Healthcare lawyers are asked to evaluate and structure transactions in a manner that considers both the business aspects and the clinical aspects of a medical practice. When advising your clients, make sure to account for the deeply rooted corporate practice of medicine doctrine in many states, which provides that practitioners, not corporations, should retain control of the business decisions that affect the practice of medicine. Recent corporate practice of medicine related cases in New York and New Jersey affirm that the doctrine is indeed alive and well.

At its core, the corporate practice doctrine prohibits non-physician owned business entities from engaging directly in clinical practice. States adopting the doctrine, whether through statutory law, common law or otherwise, commonly state that it ensures that a clinician is responsible for the control and direction of a medical practice. Many states have adopted provisions that enable healthcare professionals to enter into arm's length arrangements for services by non-physician entities. Medical professionals, however, should have an integral role in the direction of their clinical practice at all times. In transactions involving the acquisition or ownership of clinical practices, lawyers often analyze how the doctrine might impact the structure of the deal. This generally includes, but is not limited to, advice on the relationship between the various parties, structuring management agreements, setting up the corporate entity or reviewing employment agreements.

Earlier this year, in *Allstate Insurance Company vs. Northfield Medical Center et. al.*, 228 N.J. 596 (2017), the New Jersey Supreme Court affirmed a trial court's conclusion that a lawyer and a chiropractor violated the state's Insurance Fraud Prevention Act because they "promoted and assisted in the creation of a practice structure that was designed to circumvent regulatory requirements with respect to control, ownership and direction of a medical practice." While the relationships between the various parties was complex, the Court's decision centered on whether a medical practice was formed in accordance with the state's corporate practice principles. A chiropractor developed a two-day seminar called "Practice Perfect" geared toward helping chiropractors set up multi-disciplinary practices with other medical professionals. A New York lawyer served as a seminar speaker, addressing the legal considerations to be considered in the "Practice Perfect" model, including the corporate practice of medicine. As part of the lawyer's presentation, he expressly advised attendees to "retain local counsel who could confirm that his model complied with local law."

Using the model set forth in the seminar, a New Jersey chiropractor incorporated a management company and a medical corporation. The medical practice was owned by a physician and the management company was owned by the chiropractor. The management company controlled the day-to-day operations of the medical practice. The physician owner had no control over any decisions made by the medical practice nor did the physician owner appear "in charge" of any of the practice profits or design. The management company had responsibility for all financial matters and had the right to seize control of the practice at any time through an undated resignation letter signed by the physician. The physician also did not have any stock in the company. The trial court found that the lawyer and the chiropractor "promoted what was essentially a lie. The business model they promoted was intended to appear to be one way and yet, in reality, be another way." The court found that the lawyer knew that as a result of "various side agreements" the medical doctor was not in control of the practice. The appellate court upheld the trial court's conclusion that the lawyer knew the regulatory requirements and promoted a practice scheme "specifically designed to circumvent those requirements while appearing compliant."

Although it did not involve an action against the lawyer, *Andrew Carothers, M.D., P.C. v. Progressive Insurance Company*, 150 A.D.3rd 192 (2017) offers another glimpse into the factors that courts consider when assessing the doctrine. The New York appellate court upheld a jury's decision that a medical practice was not entitled to insurance payments for patient care because the practice was fraudulently organized. Dr. Carothers, a radiologist, formed a professional corporation to perform MRI services at three locations in New York. While Dr. Carothers was the sole owner of the medical practice, he leased the equipment and space from a non-physician owned entity who also exercised considerable control over the daily operations of the facilities. The Court first noted that under New York law, professional service corporations must be owned and controlled by licensed professionals. Further, the Court concluded that the jury had sufficient

evidence to find that the landlord and executive secretary were "de facto" owners of the medical practice because they exercised substantial control over the business. Specifically, the equipment lease was considered "grossly inflated," the practice profits were funneled to accounts owned by the non-physicians and personnel decisions were made by the executive secretary, rather than the physician-owner of the practice. The Court found that the physician-owner lacked knowledge about the day-to-day operations and finances of the medical practice and that under the totality of the circumstances, the jury properly concluded that the physician was not involved in the management and control of the business. As a result, the Court held that the practice was fraudulently formed and not entitled to any insurance payments.

Healthcare lawyers working on medical practice deals should ensure that the transaction is structured in a manner that takes the doctrine into account and should not promote any structure that appears to circumvent or otherwise inappropriately mask the corporate practice restrictions. As demonstrated by these cases, the common theme gleaned is that in states where there is an express prohibition on the corporate practice of medicine, the medical practices must be structured in a manner that ultimately vests control in the physician-owner. Transactions should be arranged in an artful manner that addresses the following key areas:

Contractual agreements with non-physician entities for management services should demonstrate that the physician-owner possesses the power and decision making authority to govern, control and direct matters relevant to the medical practice.

Ownership in a clinical practice, transfers of stock, issuance of shares, and other practice transactions should involve a review of the state's corporate practice of medicine restrictions. Many states provide guidance on proper ownership requirements through the State Medical Board, Administrative agencies decisions, Attorney General Opinions and legal case law.

Negotiations for services with non-physicians must be made in good faith and for commercially reasonable fees.

Transactions must not interfere with the medical professional's independent judgment with respect to patient care.

Regulatory requirements for compliance with the corporate practice of medicine may vary based on the type of medical services rendered.

Oversight and knowledge of the material business operations, staff composition and finances of the practice should involve the physician-owner of the medical practice.

Leases for equipment and space are permissible as long as they reflect an arm's length relationship between the medical practice and the lessor.

Endnotes

1 Ernessa McKie is an associate with BakerHostetler, LLP in Atlanta.

A Due Diligence Checklist: Evaluating HIPAA Privacy and Security Risks in a Deal

by Greg Gaylis[1]

Introduction

The prospect of a potential deal between parties is often accompanied by the parties' mutual sense of eagerness and excitement. The deal could, for example, consist of a merger of parties for synergy or diversification, an acquisition of assets to continue a trajectory of growth, or a joint venture to share in the risk of expanding in a new field or territory. It is rare, however, for transactional parties to share the same level of enthusiasm for the arduous due diligence process. Yet, due diligence is essential to negotiating a strategic, well vetted deal, particularly with respect to anticipating and mitigating potential inheritable liabilities. Furthermore, in an era where cyber-crime and crypto currency make daily health care industry headlines, the need to assess a transactional target or partner's privacy and security programming and practices is critical. This article provides an overview of various privacy and security requirements and highlights key due diligence considerations parties should evaluate prior to signing on the dotted line.

Privacy and Security Regulations

The Health Insurance Portability and Accountability Act of 1996 "HIPAA" includes Administrative Simplification provisions that required the U.S. Department of Health and Human Services "HHS" to adopt national standards for the privacy and security of protected health information "PHI". In fulfilling this requirement, HHS adopted the HIPAA Privacy and Security Rules. The HIPAA Privacy Rule requires covered entities (*i.e.*, health care providers, health plans, and health care clearinghouses) and their business associates to apply certain safeguards to, and limit the use and disclosure of, PHI. Correspondingly, the HIPAA Security Rule establishes national standards for the security of electronic PHI "e-PHI" in accordance with HIPAA and the Health Information Technology for Economic and Clinical Health Act "HITECH" provisions of the American Recovery and Reinvestment Act of 2009 and its implementing regulations.

The HIPAA Security Rule generally requires that covered entities and their business associates maintain reasonable and appropriate administrative, technical, and physical safeguards to protect e-PHI. More specifically, covered entities and their business associates must: (i) ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain, or transmit, (ii) protect against reasonably anticipated threats to the security or integrity of the e-PHI, (iii) protect against reasonably anticipated impermissible uses or disclosures of such e-PHI, and (iv) ensure that members of their workforce comply with Security Rule standards. Although the HIPAA Security Rule offers some flexibility to covered entities and their business associates in determining and implementing solutions appropriate for their respective circumstances (*e.g.*, size, complexity, technical infrastructure, and resources of the organization), there are certain specifications that must be implemented ("required" specifications) and others that are labeled "addressable," meaning that the covered entity or business associate must assess whether the addressable implementation specification is "reasonable and appropriate" in its environment and, if the entity determines that the specification is in fact reasonable and appropriate, then the entity must implement it.

Administrative, Physical, and Technical Safeguards

Amongst other obligations, the HIPAA Security Rule requires that a covered entity or business associate perform a risk analysis to ascertain potential risks and vulnerabilities to the confidentiality, integrity, and availability of its e-PHI, and implement security measures to reduce such risks and vulnerabilities to a "reasonable and appropriate level." Furthermore, not only are documenting and updating risk assessments compulsory under the HIPAA Security Rule, but these activities also serve as a great resource in evaluating a prospective partner's or target company's privacy and security compliance infrastructure and adherence to applicable policies and procedures (*e.g.*, updating the assessment as needed and in response to environmental and operational changes affecting the security of e-PHI).

The HIPAA Security Rule also requires covered entities and business associates to comply with the following four standards concerning physical safeguards: (i) create, implement, and maintain policies and procedures to limit physical access to e-PHI and the facilities in which they are housed, (ii) create, implement, and maintain policies and procedures that specify proper use of and access to workstations that can access e-PHI, (iii) implement and maintain physical safeguards for all workstations that access e-PHI, and (iv) create, implement, and maintain policies and procedures that govern the receipt and removal of hardware and electronic media that contain e-PHI into and out of a facility and the movement of these items within the facility.

With respect to technical safeguards, the HIPAA Security Rule requires covered entities and their business associates to comport with the following standards: (i)

create, implement, and maintain policies and procedures that allow only authorized persons or software programs to access e-PHI, (ii) develop and implement technical security measures to guard against unauthorized access to e-PHI that is being transmitted over an electronic communications network, (iii) develop and implement audit mechanisms that record and examine access and other activity in information systems that contain or use e-PHI, (iv) create, implement, and maintain policies and procedures to protect e-PHI from improper alterations or destruction, and (v) create, implement, and maintain procedures that provide for the verification of the identity of a person or entity seeking access to e-PHI. Notably, with respect to the first two technical standards (concerning access control and transmission security), the HIPAA Security Rule provides that encryption is an "addressable" implementation specification, meaning that encryption is not per se required if the entity can document that encryption is not "reasonable and appropriate" based on the entity's particular circumstances. In reality, however, HHS' Office for Civil Rights ("OCR") appears to view encryption as an operational standard of care. This position is evidenced by OCR's continued enforcement actions against covered entities and business associates for breaches involving unencrypted data. Moreover, HHS has indicated that encryption serves as a safe harbor with respect to data breaches, meaning that breach notification is not required if encrypted e-PHI is impermissibly used or disclosed (though the agency may alter this approach in the future). As such, it is important to recognize that addressable does not mean "optional." However, the passage of time and advancement in technology may blur the line between addressable and required standards.

Due Diligence: Caution of Security Risks

When leasing or buying a car, or downloading software on a computer, how many of us actually sit down to read the fine print prior to executing the transaction? In all likelihood, not many (*attorneys included*). But this norm is not the recommended approach in conducting due diligence of a prospective business partner or target company. Rather, due diligence is a critical component in gaining a comprehensive understanding of an entity's business, assets, and actual and potential liabilities.

As health care data continues to boom and the industry attracts more attention (especially negative press), proper due diligence of a prospective business partner's or target company's privacy and security infrastructure and information is becoming increasingly important. As such, the first step in the review process is to develop a complete understanding of the entity's business, such as: (i) primary and secondary business lines, (ii) size, (iii) resources, (iv) complexity, (v) capabilities, (vi) technical, hardware, and software infrastructure, and (vii) nature of individually identifiable information (including PHI) created, received, transmitted, and/or maintained by the entity.

A review strategy for privacy and security due diligence should be tailored to a particular business partner or target company, and based on the type of transaction and structure of the deal (*e.g.,* purchase of assets or stock). With this in mind, the following list, while not exhaustive, identifies several important areas parties might want to consider incorporating into their privacy and security due diligence review:

Area of Focus and Key Considerations

Data Evaluation

- Types of individually identifiable information (financial, educational, health, clinical research, tax, minor (under 18) or child (13 or under)).
- Query whether particularly sensitive or regulated data is created, received, transmitted, and/or maintained (e.g., AIDS/HIV status, psychotherapy notes, substance abuse status).
- Identify consents and authorizations (e.g., HIPAA authorizations).
- Query the entity's authority to de-identify and/or use de-identified information.
- Data storage locations (local, regional data warehouse, or offshore).

Data Flowcharts and Maps

- Request documentation as to where and how individually identifiable information is created, received, transmitted, and/or maintained.
- List all business associates and their subcontractors over the last six years.

Risk Assessments

- HIPAA risk assessments (over the last three to six years) and corrective action plans, if any.

Policies and Procedures

- Developed, documented, and current policies and procedures.
- Determine whether the policies and procedures were distributed to staff, and whether the staff members were given adequate and recurring training and education.
- Compliance with applicable laws, regulations, and payor-specific requirements.

Network Security and Physical Security

- Penetration and vulnerability testing history.
- Staffing and training for security monitoring, phishing, ransomware, and breach responses.
- Firewall adequacy, encryption technology, data in motion safeguards (e.g., VPN).
- Review physical security policies, procedures, training, and assessments.

Contracts and Contract Management

- Review template/executed business associate and subcontractor business associate agreements, data use agreements, ancillary data agreements, and contract management arrangements.

Privacy and Security Compliance Program

- Validate occurrence of HIPAA training, and review internal/external investigations, HIPAA privacy or security incident claims or breaches, security incident protocols, corrective action plans and other risk mitigation documentation, and record retention policies and procedures.

Breach Reporting

- Request a list and copies of notices to HHS, federal and state agencies, and individuals for all HIPAA breaches within the last six years.

Government Investigations and Enforcement History

- Determine whether the entity is or has been the subject or target of prior government investigations with respect to a privacy or security incident.
- Review history of government enforcement, if any (e.g., settlements or corrective action plans).

Private Claims/Actions

- Probe whether the entity has been subject to private litigation due to a privacy or security incident.

Conclusion

Once the parties complete due diligence, they must determine how to effectively address both actual and potential risks and liabilities. Mitigation of such risks and liabilities can be negotiated through several means. Common risk mitigation strategies include, for example, negotiating representations and warranties in the transactional documents to account for identified and anticipated liabilities, requiring representations and warranties insurance (a relatively new type of insurance designed to cover the liability associated with a breach of a representation or warranty contained in a transaction document), ensuring protection through indemnification, requiring occurrence-based insurance policies, reducing the purchase price or capitalization contributions or pursuing an asset only deal, holding funds in an escrow account to resolve such liabilities should they come to fruition following the transaction, and requiring privacy and/or cyber security insurance (a burgeoning branch of the insurance market with strenuous requirements by the insurer to qualify for coverage).

Endnotes

1. Greg Gaylis is an Associate in the Health Care Practice at Dentons, US LLP.
2. Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191, 110 Stat 1936 (1996).
3. 45 C.F.R. Part 160 and Subparts A and E of Part 164.
4. 45 C.F.R. Part 160 and Subparts A and C of Part 164.
5. See Subpart C of 45 C.F.R. Part 164.
6. 45 C.F.R. § 164.306(a).
7. 45 C.F.R. § 164.306(d).
8. 45 C.F.R. § 164.308(a)(1).
9. 45 C.F.R. §164.306(e), 45 C.F.R. §164.316(b).
10. 45 C.F.R. § 164.310.
11. 45 C.F.R. § 164.312.

Health Law Developments is looking for authors of new content for publication.

If you would like to contribute an article or have an idea for content, please email Keri F. Conley at kconley@gha.org.

Cybersecurity Risk in Health Care[1]

by Barry S. Herrin[2]

Abstract

The need for constant availability and integrity of patient data means that many organizations compromise on privacy and security, often to their detriment. This article discusses the current state of healthcare data privacy and security, examines the legal issues requiring attention, discusses risks of the growing use of remote technologies, mHealth and wearable technology, and finally discusses cybersecurity insurance as a way to mitigate the financial costs of breach.

The Current State

Notwithstanding the imperative of the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its Privacy and Security Rule,[3] the era of interoperability has created a de-emphasis on the confidentiality of medical information while, at the same time, creating a tremendous emphasis on integrity and availability.

Findings from the Health Care Industry Cybersecurity Task Force in its final report of June 2, 2017[4] show that, "of the three aims of cybersecurity (confidentiality, integrity, availability), availability is the most important. You cannot take care of patients without having availability of information. Having high availability of patient information is especially important with hospitals that operate 24x7 and 365 days a year." Second to availability was integrity of data. The HCIC report specifically stated that "integrity of data is important for protecting patient safety," which is "directly implicated when it comes to connected medical devices and patients whose health can be directly impacted by the operation of the medical device." However, the report recognizes that the drive to interoperability has resulted in the confidentiality of medical information being de-prioritized and asserts that "healthcare data confidentiality must remain top of mind."

A 2017 KLAS survey reports that 41 percent of respondents said their health systems dedicate less than three percent of the IT budget to cybersecurity, primarily because IT leadership has been focused on implementing electronic health record systems and dealing with interoperability challenges.[5]

Task Force Imperative four calls for an "increase [in] healthcare industry readiness through improved cybersecurity awareness and education." However, the increase in readiness "requires a holistic cybersecurity strategy. Organizations that do not adopt a holistic strategy not only put their data, organizations, and reputation at risk, but also—most importantly—the welfare and safety of their patients."

In the healthcare industry specifically, the financial impact of cybersecurity breaches is grim. One in three Americans were affected by healthcare breaches in 2015, according to a report from Bitglass.[6] That's more than 113 million individuals. Each lost or stolen medical record costs a healthcare organization $363 per record on average, per a Ponemon Institute report.[7] The anecdotal record is not any more pleasant: Hollywood Presbyterian's information systems were held hostage in Feb. 2016 for $3.6 million in Bitcoin,[8] and more and more healthcare enterprises are creating reserves for data ransom. A 2016 IBM study quoted by *SC Media UK* showed that, in the United States, 70 percent of businesses receiving a ransomware demand paid to get their data back, with 50 percent of those paying more than $10,000 and a further 20 percent paying more than $40,000.[9]

No matter the technology used in the healthcare industry today—e-signature software, EHR platforms, wearable devices, smartphones, tablets, or other software or hardware—providers can either work to mitigate risk or watch the organization spiral into potentially uncontrollable vulnerability. Today's electronic environment leaves little room for laissez-faire security efforts if a healthcare provider wants to remain safe from attack and protected from the financial consequences of the inevitable.

Why HIPAA Still Matters

HIPAA in general, and the Security Rule in particular, imposes specific compliance burdens on healthcare "covered entities." Any use or disclosure of electronic protected health information (ePHI) not in compliance with the Privacy and Security Rules or more stringent state law constitutes a violation of HIPAA.[10] The failure of a covered entity to implement sufficient security measures regarding the transmission of and storage of ePHI to "reduce risks and vulnerabilities to a reasonable and appropriate level" is also a violation.[11] Likewise, a failure to implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain ePHI into and out of its facility, and the movement of these items within its facility, are violations.[12] And, once a security incident occurs, the failure to "timely identify and respond to a known security incident, mitigate the harmful effects of the security incident, and document the security incident and its outcome" are all violations.[13]

At the time of writing, most of the Security Rule fines and penalties assessed by the US Department of Health and Human Services Office for Civil Rights (OCR) relate solely or primarily to either (1) theft of devices containing unsecured ePHI or (2) failure to conduct a security risk assessment that is discovered when another privacy or security breach is investigated. Examples of such "traditional" enforcement activity in recent times include the August 2015 announcement of a $750,000 settlement against Cancer Care Group, P.C. for the theft of an employee laptop containing ePHI on 55,000 individuals, the December 2013 announcement of a $150,000 settlement against Adult & Pediatric Dermatology, P.C. for the theft of a thumb drive containing ePHI on 2,200 patients, and the

announcement of settlements by Idaho State University and University of Washington Medicine for failure to conduct privacy and security risk assessments and failure to adequately adopt security measures. Were this still the level of involvement by OCR in ePHI enforcement, a shrug of the CIO's shoulders and a promise to encrypt all ePHI data at rest would be the universal response.

However, in recent times the enforcement focus has shifted to more "core" system security functions and away from the "low hanging fruit" of lost or stolen data-carrying devices. For example, a $850,000 settlement paid by Lahey Clinic Hospital in 2015 specifically references the failure "to assign a unique user name for identifying and tracking user identity" with respect to a particular workstation,[14] failure to have a working audit trail capability with respect to workstation activity,[15] and the failure to restrict physical access to workstations generally to authorized personnel. A similar enforcement activity against South Broward Hospital District in February 2017 resulted in a $5,500,00 settlement payment based on improper access to ePHI by over a dozen individuals exposing in excess of 80,000 patient records and the failure of the covered entity to "implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports"[16] and "to implement policies and procedures that establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process."[17] Several enforcement activities also resulted in settlements for failure to have business associate agreements in place with third-party vendors responsible for storing ePHI.[18] Just as the environment for bad cyber behavior has matured, so has the OCR's level of understanding of system and enterprise failures of the healthcare community.

The Healthcare Internet of Things

The task of HIPAA compliance and compliance with cybersecurity "best practices" is being made harder with the proliferation of Internet-connected devices in the healthcare industry. As recently as 2012, a Ponemon Institute survey reported that 69 percent of respondents did not even address the security of US Food and Drug Administration (FDA) approved medical devices in their IT security or data protection activities.[19] Since that time, over five billion devices—*not including smartphones*—have connected to the Internet, and that number is expected to grow to between 25 billion and 50 billion by 2025.[20]

The healthcare industry has particular patient safety risks associated with these devices, as revealed in a 2012 US Government Accountability Office report on the lack of action by the FDA to expand its consideration of information security for medical devices.[21] A November 2015 Wired.com survey listed the seven healthcare device types most vulnerable to hacking or other violation which included drug infusion pumps, Bluetooth-enabled defibrillators, blood refrigeration units, and CT scanners—the failure of any of which would create tremendous patient risk. We have grown far beyond the fear of hacking the vice president's pacemaker.[22]

The fact that smartphones are not included in this total is worrisome, as the growth in potential cyber risk due to smartphone use is even more troubling. 84 percent of health applications for smartphones that were approved by the FDA were found to create HIPAA violations and were "hackable."[23] Also worrisome is the continued increase in the use of smartphones to transmit and receive unsecured ePHI (primarily by text message) for patient treatment by healthcare professionals, in spite of HIPAA's requirements and facility rules attempting to limit such activity.[24] Most health care enterprises gave up the fight over "bring your own device," or BYOD, rules due to provider pressure a long time ago anyway. Although study results vary, as of 2014 "upward of 90 percent of healthcare organizations permit employees and clinicians to use their own mobile devices to connect to a provider's network or enterprise systems."[25]

One has to wonder what OCR's response to all of this would be in light of the settlement agreements mentioned earlier: the decision not to impose device accountability for provider convenience may be fertile ground for future fines and penalties. And there is always the modern privacy paradox: health care consumers voluntarily share endless amounts of personal health information with applications on their smartphones, resulting in data being stored who-knows-where on the Internet without them thinking if it is convenient for them[26]; however, these same consumers continue to resist the same sharing activities by their own healthcare providers, even if such activity would result in faster and better health care.[27]

Cybersecurity Insurance

In October of 2002, *The Economist* magazine opined[28] that "total security was impossible" and that insurance would be the way that businesses mitigated the financial risk caused by this lack of security. Since that time, both security defenses and security attacks have proliferated, changed, and become more aggressive and complex. However, the cybersecurity insurance market, though maturing, is not developing at as rapid a pace. Some issues that remain to be explored are due to the relative newness of the coverage and the lack of good predictive actuarial models.[29]

While the market matures, there are various factors that potential insureds should evaluate closely as they shop for and price out cybersecurity insurance. The first and most important of these coverages should be the coverage of costs related to managing breaches, to include expenses related to the investigation, remediation efforts, and patient notification. Other costs that may also be incurred are credit monitoring services,[30] damages associated with identity theft, damages associated with recovery of data, damages incurred due to having to reset EHR systems, and damages to reconstruct or recover websites and other Internet presences. Business continuity expenses related to workarounds or loss of revenue due to a cybersecurity incident might also need coverage, especially as most commercial policies of this type are figuring out how to exclude cyber-related risks from their covered losses. Finally, but not least importantly, coverage for rogue employees and insider threats needs to be a part of the insurance package.

The type of coverage a healthcare enterprise can obtain, and the premiums therefor, may be affected by certain underwriting considerations, all of which should inform the enterprise's compliance efforts:

- The enterprise should be able to show that it is in compliance with HIPAA, including those provisions that require security and privacy risk assessments and proof of a plan of mitigation and remediation. Insurers likely will not cover losses resulting from a gap in HIPAA compliance, especially because there is a legal obligation on the enterprise to find out what those are.
- The potential insured needs to know what the insurer's requirements are for encryption beyond those mandated by HIPAA. Some coverages require more secure and more robust email systems that are more resistant to phishing and spoofing, and even other coverages may require intentional phishing attacks by the insured's IT department or vendors to gauge compliance with training.
- The training requirements for new employee onboarding and access by non-employee contractors may need to meet certain criteria beyond HIPAA workforce awareness training.
- Insurers may require that contractors providing "business associate" services be separately insured as a first layer of defense against cost.
- The potential purchaser needs to be on the lookout for what is referred to in the industry as "cannibalizing" coverage, in which the costs of defense reduce the limits available to pay damages or judgments. The best coverage separates costs of defense from claims expenses.
- The purchased coverage, as with certain types of malpractice insurance, should be based on the "date of detection" as opposed to "date of intrusion." It is so difficult, even with the best system monitoring tools, to determine when a breach or incident actually first occurred, so the enterprise does not want to be locked into a technical dispute with the insurer about when the hack "should have been" detected.
- The prospective insured needs to know whether offshore operations will be covered. Significant risks are associated with outsourcing certain data manipulation and management functions to countries or regions that have stronger privacy and data security rules than the United States. In particular, the European Union takes a dim view of American-style discovery and most likely will not permit the compelled return of data from an EU vendor in litigation pending in United States courts.

Conclusions

The growth of connected devices, connected physicians, and connected patients will continue to push healthcare facilities to provide more interoperability for health data than ever before. These same technological pressures will make it easier for cybercriminals and disgruntled employees to compromise the data upon which everyone relies for reliable patient care, because an increase in interoperability in most cases creates an increase in gaps in security. Healthcare systems need to recognize this risk as a direct threat to patient care, and not just to its financial and technology resources. A holistic security approach, combining effective cybersecurity practices, HIPAA training and compliance, and appropriate insurance coverages will be the best way to address this growing area of opportunity—and risk—in the future.

Endnotes

1. Originally published in the September 2017 ISSA Journal, the monthly publication of the Information Systems Security Association (ISSA) – Developing and Connecting Cybersecurity Leaders Globally – www.issa.org/?page=ISSAJournal. Reprinted with permission.
2. Barry S. Herrin, JD, FAHIMA, FACHE, is the founder of Herrin Health Law P.C. in Atlanta, Georgia. Herrin has over 25 years of experience practicing law in the areas of healthcare and hospital law and policy, privacy law and health information management, among other healthcare-specific practice areas. He is both a Fellow of the American College of Healthcare Executives and a Fellow of the American Health Information Management Association and holds a Certificate in Cyber Security from the Georgia Institute of Technology. He may be reached at http://barry.herrin@herrinhealthlaw.com.
3. 45 CFR Parts 160 and 164; the enabling legislation is found at 42 U.S.C. Section 1320a-7c.
4. "Report on Improving Cybersecurity in the Health Care Industry," Health Care Industry Cybersecurity Task Force (June 2017) – https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf.
5. Center for Connected Medicine report, "The Internet of Medical Things: Harnessing IoMT for Value-Based Care," July 2017 – https://www.connectedmed.com/files/assets/common/downloads/publication.pdf.
6. Bitglass. "Bitglass Healthcare Breach Report 2016," Bitglass – https://pages.bitglass.com/BR-Healthcare-Breach-Report-2016_PDF.html.
7. Larry Ponemon, "Cost of Data Breaches Rising Globally, Says '2015 Cost of a Data Breach Study: Global Analysis,' " Security Intelligence, May 27, 2015 – https://securityintelligence.com/cost-of-a-data-breach-2015.
8. Vincent Lanaria, "Hackers Hold Hollywood Hospital's Computer System Hostage, Demand $3.6 Million As Patients Transferred," Tech Times, 16 February 2016 – http://www.techtimes.com/articles/133874/20160216/hackers-hold-hollywood-hospital-s-computer-system-hostage-demand-3-6-million-as-patients-transferred.htm. The hospital eventually paid $17,000 in Bitcoin.
9. Max Metzger, "Your Money or Your Files: Why Do Ransomware Victims Pay Up?" SC Magazine UK, May 25, 2017 – https://www.scmagazineuk.com/your-money-or-your-files-why-do-ransomware-victims-pay-up/article/664211/.
10. 45 C.F.R. §§ 160.103 and 164.502 (a). NOTE: CFR 45, Parts 160 and 164 can be found at US Electronic Code of Federal Regulations: Title 45—Public Welfare, Subchapter C—Administrative Data Standards and Related Requirements: 160-164 – https://www.ecfr.gov/cgi-bin/text-idx?SID=fbc57ba7be313c69e19aa1e78ac97adf&mc=true&tpl=/ecfrbrowse/Title45/45CsubchapC.tpl.
11. 45 C.F.R. §164.308(a)(1)(ii)(B)
12. 45 C.F.R. § 164.310(d)(1)
13. 45 C.F.R. § 164.308(a)(6)(ii)
14. 45 C.F.R. § 164.312(a)(2)(i)
15. 45 C.F.R. § 164.312(b)

16. 45 C.F.R. §164.308(a)(l)(ii)(D)
17. 45 C.F.R. § 164.308(a)(4)(ii)(C)
18. As examples, see the July 18, 2016 Resolution Agreement with Oregon Health & Science University in which $2,7 million was paid and the September 23, 2016 Resolution Agreement with Care New England Health System in which $400,000 was paid.
19. John Glaser, "The Risky Business of Information Security: With Growing Threats to Patient Privacy and Increasing Sanctions by Regulators, Make Data Security Central to Your Business," Hospitals & Health Networks, August 12, 2014 – http://www.hhnmag.com/articles/4064-the-risky-business-of-information-security.
20. The Florida Bar, "8th Annual FUNdamentals: The Legal Implications of the 'Internet of Things'," Course 2232R (September 16, 2016)
21. GAO, "Report to Congressional Requesters: Medical Devices: FDA Should Expand Its Consideration of Information Security for Certain Types of Devices," United States Government Accountability Office, August 2012 – http://www.gao.gov/assets/650/647767.pdf.
22. Lisa Vaas, "Doctors Disabled Wireless in Dick Cheney's Pacemaker to Thwart Hacking," Naked Security, Sophos, 22 Oct 2013 https://nakedsecurity.sophos.com/2013/10/22/doctors-disabled-wireless-in-dick-cheneys-pacemaker-to-thwart-hacking/.
23. Ibid.
24. Ibid. (citing a 2015 University of Chicago survey finding that over 70 percent of its medical residents improperly sent ePHI by text messages).
25. John Glaser, "The Risky Business of Information Security: With Growing Threats to Patient Privacy and Increasing Sanctions by Regulators, Make Data Security Central to Your Business," Hospitals & Health Networks, August 12, 2014 – http://www.hhnmag.com/articles/4064-the-risky-business-of-information-security.
26. Shannon Barnet, "Millennials and Healthcare: 25 Things to Know," Becker's Hospital Review, August 04, 2015 – http://www.beckershospitalreview.com/hospital-management-administration/millennials-and-healthcare-25-things-to-know.html. 71 percent of Millenials surveyed by Harris would use a mobile app to share health care data with providers. See also Mintel, "Sixty Percent of Millennials Willing to Share Personal Info with Brands," Mintel, March 7, 2014 – http://www.mintel.com/press-centre/social-and-lifestyle/millennials-share-personal-info, in which the study reports that 60% of Millennials would be willing to provide details about their personal preferences and habits to marketers, and, of those that would not initially provide such information, 30% would do so after receiving an incentive offer such as a discount off future purchases.
27. Denver Nicks, "Survey: Millennials Care about Privacy (But Not So Much in Japan), Time, Nov. 07, 2013 – http://techland.time.com/2013/11/07/survey-millennials-care-about-privacy-but-not-so-much-in-japan/. Only 4% of respondents would be comfortable with data being used for a purpose outside of its original context. The study also says that these preferences vary by economic status, with high-income worried more about data privacy than low-income people.
28. "Putting It All Together," The Economist (October 24, 2002)
29. Koo, "More Incident Data Needed for Cybersecurity Insurance," Bloomberg BNA (March 28, 2016)
30. Even though there is almost a universal recognition in the law enforcement and security communities that these programs do no good at all, as the sophisticated hacker knows to wait out the 1-2 years of service before making use of the stolen data.

Advanced Health Law Seminar

On Oct. 20, 2017, we held our annual Advanced Health Care Law Seminar at the Four Seasons Hotel in Atlanta. During the program, about 150 attendees networked with members of Georgia's health care community and attended presentations given by local and national leaders in various areas of health law. Presentation topics included Medicaid reform, telemedicine, privacy and security, post-acute care, fraud and abuse and opioid abuse. Additionally, Frank Berry, Commissioner of the Georgia Department of Community Health delivered the keynote speech, highlighting the department's points of focus and plans for the future.

Immediate Past Chair Keith Mauriello

Commissioner Frank Berry

Chair Lynn Adam

Privacy and Security Panelists

Health Law Developments is looking for authors of scholarly articles. If you have an article to submit, please contact Rebecca Merrill at rebecca.merrill@dentons.com

Farewell Message

Dear Health Law Section Members,

I write this as my farewell as the Health Section Chair and would like to start by wishing all of you Happy New Year! It has been a pleasure and honor to serve as the Chair, and I am amazed at how much our Section has accomplished over this past year. Such success would not have been possible without our dedicated and fantastic Executive Committee. Thanks to each of them for a terrific job and for all of their support and efforts. We are also in great hands with the new slate of Officers, with Lynn Adam as the new chair, and I know that this coming year will be better than last and that the Executive Committee will continue to work in the right direction to better serve the Section. Thank you again.

Best in 2018, Keith Mauriello

Past Health Law Section Chairs

Keith Mauriello
Daniel J. Mohan
Mark Stuart Kashdan
Brian McEvoy
Summer Martin
James Boswell
Robert Stone
Charlotte Combre
Tracy Field
Robert Porter Jr.
Kathy Butler Polvino
Lori Spencer
William W. Calhoun
Rod G. Meadows
Jeffrey Baxter
Jonathan Lee Rue
Charlene L. McGinty
Kevin E. Grady
Paul G. Justice
Charity Scott
Eve H. Goldstein
Randall L. Hughes
G. Richard Langley
James R. McGibbon