OPERATIONAL RISKS TO A SUCCESSFUL PHYSICIAN SPECIALIST

ISSUES AND POTENTIAL SOLUTIONS

TSATSATZU
BOSTON, MA USA
2015

The Client

The Client is a physician specialist operating several independent offices in Metropolitan Boston. His professional credentials and peer standing are excellent. He has privileges at teaching hospitals and an enormous clientele of largely white, upper middle class patients. His hourly rate is in the $600-800 range while office expenses – staff, square footage – are minimal. He carries top-of-the-line tiered malpractice insurance, and he has excellent relationships with the major health insurance providers in the area. His daily client roster does not appear to impact his professional competence, health or well-being.

In effect the Client has built a so-called "Cash Machine for Life," a well-built professional practice anchored in his expertise and connections. He has protected against certain operational risks, by diversifying his patient load, by negotiating with major health insurance providers and investing in malpractice insurance. The question is whether other operational risks have been overlooked, and if so, what actions might be taken to harden the business and it revenue stream against such threats.

The Initial Assessment

The consulting engagement will consist of several phases. The initial phase has been limited to assessing the operational risks which have not already been addressed by the business, that is, activities or procedures which could endanger the business as a whole. Our initial assessment recommends addressing three specific kinds of operational risk:

1. HIPAA Compliance Risk
2. Licensure/Insurance Risk
3. Physical Safety Risk

The following paragraphs define these risks and raise questions regarding current business practices and methods, which could bring these risks to bear on the long-term viability of the business.

HIPAA Compliance Risk

The Health Insurance Portability and Accountability Act (HIPAA) is a federal law (Public Law 104-191) passed by Congress in 1996. The HIPAA Privacy Rule (45 CFR Parts 160 and 164) provides the first comprehensive Federal protection for the privacy of health and mental health information. The Rule is intended to provide strong legal protections to ensure the privacy of individual health information, without interfering with patient access to treatment, health care operations, or quality of care. The Privacy Rule specifically protects all "protected health information" (PHI), including individually identifiable health or mental health information held or transmitted by a covered entity in any format, including electronic, paper, or oral statements.[1]

[1] New York State Office of Mental Health, HIPPA Privacy Rules for the Protection of Health and Mental Health Information, collected March 2015.

HIPAA places the burden of compliance upon the healthcare provider. In the case of a physician specialist, he is responsible for protecting the privacy of all digital communications. Email, chat and videoconferencing software all fall within the purview of this law. From the Department of Health & Human Services (HHS) website:

> *The Security Rule does not expressly prohibit the use of email for sending e-PHI. However, the standards for access control (45 CFR § 164.312(a)), integrity (45 CFR § 164.312(c)(1)), and transmission security (45 CFR § 164.312(e)(1)) require covered entities to implement policies and procedures to restrict access to, protect the integrity of, and guard against unauthorized access to e-PHI. The standard for transmission security (§ 164.312(e)) also includes addressable specifications for integrity controls and encryption. This means that the covered entity must assess its use of open networks, identify the available and appropriate means to protect e-PHI as it is transmitted, select a solution, and document the decision. The Security Rule allows for e-PHI to be sent over an electronic open network as long as it is adequately protected.*[2]

In addition, the healthcare provider is responsible for the security of all laptops and other portable and/or mobile devices, which are required to also be in compliance with the HIPAA Security Rule. This requirement applies to organizations that allow remote access to e-PHI through portable devices or on external systems or hardware not owned or managed by the covered entity.[3]

Lastly the HIPAA Security Rule requires the reviewing and modifying, where necessary, of security policies and procedures on a regular basis. Further documentation from the HIPAA site includes details on schedules and quality standards.[4]

Questions

- *Are all physician-patient communications – email, chat, videoconferencing, etc. – HIPAA secure; i.e., protected by third-party encryption?*
- *Are patients routinely being made aware of their HIPAA rights as part of intake?*
- *When are HIPAA protocols being reviewed? And by whom?*
- *What protections are in place against the interception of doctor-patient communications? Is hacking of concern?*
- *Could patients waive their privacy rights, either implicitly or explicitly, to unnamed third parties? What does the CVS example*[5] *suggest?*

[2] Department of Health & Human Services, "Does the Security Rule allow for sending electronic PHI (e-PHI) in an email or over the Internet. If so, what protections must be applied?" hhs.gov, collected 2015.
[3] Department of Health & Human Services, "HIPAA Security Guidance", hhs.gov, collected 2015.
[4] HIPAA Security Series, "2 Security Standards: Administrative Safeguards," hhs.gov, collected May 2015.
[5] Patrick Ouellette, "Privacy and security experts respond to CVS HIPAA waivers," Health IT Security, August 22, 2013.

MEDICAL REVIEW BOARD/INSURANCE

Under Massachusetts law, a physician must maintain adequate records for each patient, and retain the record for at least seven years from the date of the last encounter with the patient or until the patient reaches the age of nine (if more than seven years).[6] All providers (defined as "individual, group, facility, agency, institution, organization, or business that furnishes medical services and participates in MassHealth") must keep documentation of the services provided under MassHealth, including medical records, to disclose the extent of and medical necessity of the services provided. Providers must also maintain patient account records, which completely document charges, indicate debits and credits, and show the amounts billed and paid.[7]

Likewise, the Centers for Medicare and Medicaid Services (CMS), which controls 35% of national health expenditures as of 2013[8], requires its payees to include detailed clinical notes to justify covered services. Furthermore, the CMS' renewed focus on Clinical Quality Measures (CQMs) has intensified the expectation for documentation.[9]

Private payers, which control another 33% of the market, have similar expectations for recordkeeping and are more likely to demand proof for payment of services. From the Massachusetts Medical Society,

> *Physicians are more vulnerable to payer audits and payment recoupments than ever. Public and commercial payers audit physician practices of all sizes, and physicians can minimize the impact by being prepared and thoroughly documenting each patient encounter. If the service is not documented appropriately, the auditor or investigator may find that the service provided or the level of service billed was not justified, therefore resulting in a payment recoupment, or takeback.*[10]

Such outcomes highlight the importance of staving off audit or being prepared to address requests for audits from any private payer accepted within the specialty practice.

Questions

- *Are patient clinical records clear, accessible, up-to-date and consistent with licensing and third-party payer standards?*
- *Is the physician readily able to verify patients' diagnoses, prescriptions and clinical plans in case of treatment failure?*
- *Are patient records available to re-issue prescriptions, protect against claims of negligence and/or address third-party claims?*
- *In the case of a patient who received the wrong medication, would the main evidence rest with the prescribing pharmacy? Or would prescriber records include a paper trail?*

---

[6] "Medical Records Collection, Retention and Access in Massachusetts,"HealthInfoLaw.com (243 MA ADC 2.07(13)(a)-(b).
[7] Ibid. 130 MA ADC 410.409.
[8] NHE Factsheet, www.cms.gov , collected May 2015.
[9] Clinical Quality Measure Basics, CMS.gov, collected May 2015.
[10] Talia Goldsmith, "Three Action Steps for Physicians Facing Payer Audits or Recoupment," Massachusetts Medical Society, March 2015.

- *What if a patient needed new or additional medicine, having never filled a previous prescription? Would the prescriber have the clinical records to support clinical judgment?*
- *Is insurance coverage predicated upon specific recordkeeping procedures?*
  Is HIPAA compliance a requirement of coverage? Is coverage contingent on HIPAA compliance?
  In the event of a data breach of private health data, how much does insurance protect against claims, especially damages?

PHYSICAL SAFETY

The sad fate of cardiac surgeon Michael J. Davidson of Brigham & Women's Hospital (BWH) has forced physician specialists in many fields to re-examine their physical safety within their work environments. BWH or "The Brigham" had prepared its staff with regular training drills and had employed police details onsite, who arrived within seconds of the shooting.[11]

The incident has raised questions regarding the preparedness of other hospitals as well as physician specialist practices throughout the region. The Occupational Health & Safety Administration (OSHA) has intervened in certain instances to ensure minimum safety standard protocols are in place to protect medical staff.[12] The U.S. Bureau of Labor Statistics notes that nearly 60% of all non-fatal assaults and violent acts occurred in the health care and social assistance industry and that "…a worker in health care and social assistance is nearly five times more likely to be the victim of a nonfatal assault or violent act a by person than the average worker in all other industries combined."[13] RatesThe frequency of physical assault on medical personnel by patients suffering from mental health issues is of particular concern:

> *According to the United States Department of Justice's National Crime Victimization Survey conducted from 1993 to 1999, the annual rate of nonfatal, job-related violent crime was 12.6 per 1,000 workers in all occupations. Among physicians, the rate was 16.2 per 1,000, and among nurses, 21.9 per 1,000. However, for psychiatrists and mental healthcare professionals, the rate was 68.2 per 1,000, and for mental health custodial workers, 69 per 1,000.*[14]

The specific risk faced by any particular physician specialist, such as the Client, is unknown. It is reasonable to assume, however, that the risk increases with the number of patients seen per unit of time.

Questions

- *What physical measures are in place to help defend against physical threats?*

---

[11] Jessica Barlett, "Brigham shooting sheds new light on hospital violence legislation," *Boston Business Journal*, Jan 21, 2015 3:21 pm EST.
[12] *Ibid.*
[13] Jill A. Janocha and Ryan T. Smith, U.S. Bureau of Labor Statistics, "Workplace Safety and Health in the Health Care and Social Assistance Industry, 2003-07," August 30, 2010.
[14] Friedman RA. Violence and mental illness: how strong is the link? N Engl J Med. 2006;355:2064–2066. [PubMed]

    - *Are emergency (aka panic) buttons in place? How quickly will help respond?*
    - *Are doors reinforced? Are fire ladders available in all upper story rooms?*
    - *Are escape routes easily accessed throughout the office?*
- *What offensive protections are already in place?*
    - *Are any weapons on hand? Are they securely stored?*
    - *Are guards in place to monitor entrances and exits? Do they check on the office regularly?*
- *What protocol measures have been put in place to enhance the physical safety of the office?*
    - *Is an evacuation plan in place?*
    - *Does staff practice dealing with emergency situations on a regular schedule?*
    - *Has staff practiced accessing weapons in simulated emergency situations?*
- *What would happen if a patient with significant and/or unmanaged mental health issues became violent at an office?*

Recommendations

Each physician specialist faces unique risks in his or her practice as a natural consequence of the delivery of healthcare services in an increasingly competitive marketplace. The key is to identify unaddressed operational risks and assess their potential impacts, according to their likelihood and severity.

The Client provides an excellent level of care to a steady stream of patients. The next step is to prioritize these risks according to which pose the greatest threat; i.e., have the strongest likelihood of occurring and/or carry the most severe consequences. The following recommendations summarize general options towards addressing these risks without prioritizing their relative immediacy or importance.

- Implement HIPAA compliant email, chat and videoconferencing protocols.
- Establish regular reviews of HIPAA compliance practices.
- Audit clinical notes regularly to ensure compliance with recordkeeping standards for all accepted third-party payers.
- Establish procedures to maintain compliance with these recordkeeping standards.
- Contact malpractice insurers and/or risk management departments to understand riders and coverage benefits in case of audit and gauge where best to concentrate effort.
- Identify patients and/or clinical situations in which prescriptions have remained unfilled.
- Audit prescriptions for consistency with prescription fillers and medical device suppliers.
- Secure the medical offices against physical attack and upgrade means of self-protection and escape.
- Conduct routine drills to ensure that the protocols work when needed.

Next Steps

This document has outlined a framework for identifying specific areas of concern as well as potential solutions. The next step is to prioritize these risks and form plans to address them. Towards these ends, we will be convening several conversations with stakeholders to address these specific risks according to

their relative priority; i.e., their likelihood as well as their potential severity. This phase will conclude with a mutually agreed plan to address issues that endanger the business as a whole.

Once these operational risks are addressed, we will turn the focus of this consulting engagement towards improving the practice's operational efficiency: billing, scheduling, and cash cycles. We will be identifying specific technical and training issues in conjunction with their estimated impacts on the financial bottom line. We also anticipate the expansion into a third phase, where work will concentrate on expanding the Client's reputation beyond Metropolitan Boston. For this piece, we will be looking at referral channels, interstate licensing restrictions and ways to leverage his academic standing into mainstream recognition.