MIEC

The Exchange

JULY 2012 ISSUE 2

INSIDE

MIEC *The Exchange* is published by Medical Insurance Exchange of California, 6250 Claremont Avenue, Oakland CA 94618. Articles are not legal advice. Reproduction with permission. © 2012

2011 MIEC Annual Report to Policyholders

We are pleased to report that 2011 was a very successful year for MIEC. In spite of all the taxing pressures of the profession, we hope it was a good year for you and your practice. We are frequently told that being insured with MIEC continues to provide our policyholders with some certainty and comfort and that this is one thing that you don't need to worry about. We hope this is your experience.

MIEC continues to adhere to the philosophies and business objectives upon which the organization was founded – to serve our existing policyholders and deliver the best possible product at the lowest sustainable price. In 2011, we increased the dividend, added new capabilities, improved operational efficiencies, and lowered prices for a large majority of our insureds. MIEC financials have never been stronger and we are confident in our ability to fulfill the promises we make to you.

Dividends have never been higher and rates are down for most policyholders

At our December 2011 meeting the Board of Governors declared a $30m dividend – the largest in the long line of dividend declarations that have resulted in over $330m being returned to renewing policyholders over the past 3 decades. In the past 5 years, MIEC has used profits

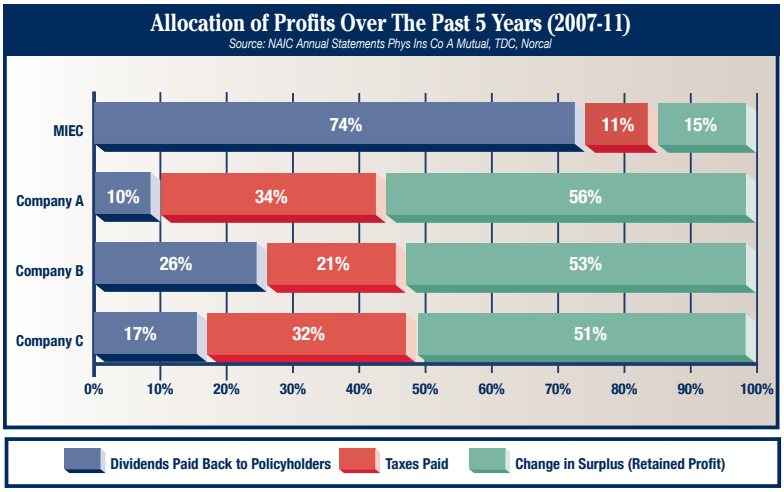

Figure 1

to offset approximately **41%** of policyholder's basic premiums.

You may not be aware that MIEC's approach to profits and dividends is highly unusual. As the data shows in ***Figure 1***, MIEC returns a vastly larger proportion of its profits to our policyholders than our close competitors: 74 cents of every dollar as compared with 10, 26 and 17 cents.

Every year, we review our pricing and make adjustments to base rates that flow through our existing pricing structure. In recent years, overall pricing has been flat or reduced depending on the state in which you practice. In 2011, the MIEC Board conducted a more extensive evaluation of all the elements of our rating structure. This is a major undertaking and is done every 5 years or so to ensure that our pricing for the different specialties we insure is reflective of their claims experience.

This review resulted in a number of changes. Overall, it produced indications for a substantial reduction in California, single digit reductions in Idaho and Alaska, and flat rates in Hawaii. The rate filings were submitted to and approved by the insurance regulators in each state and were implemented in time for the February 1st renewal.

A bigger dividend and lower rates are clearly not going to happen every year,

2011 Four Year Consolidated Financial Review

Medical Insurance Exchange of California

	2011	Percentage Change	2010	Percentage Change	2009	Percentag Change	2008
Net Admitted Assets	**$379,473,000**	**2.63%**	$369,759,000	5.87%	$349,243,000	6.01%	$329,432,000
Direct Written Premium	**$66,755,000**	**-3.48%**	$69,163,000	-3.98%	$72,030,000	-3.77%	$74,852,000
Net Written Premium	**$60,897,000**	**-10.90%**	$68,347,000	6.35%	$64,268,000	-2.16%	$65,687,000
Policyholders' Surplus	**$166,244,000**	**5.27%**	$157,927,000	8.59%	$145,434,000	17.49%	$123,785,000
Ratio: Net Written Premium to Surplus	0.37:1		0.43:1		0.44:1		0.53:1
Net Investment Income	**$27,471,000**	**-7.17%**	$29,594,000	21.24%	$24,409,000		$(20,647,000)
Invested Assets*	**$368,740,000**	**2.80%**	$358,687,000	5.27%	$340,733,000	7.07%	$318,243,000
Underwriting Gain (Loss)	**$12,405,000**		$5,609,000		$12,436,000		$32,165,000
Dividends Declared	**$30,000,000**		$25,000,000		$20,600,000		$17,000,000
Total Dividends Declared Since Inception	**$331,675,000**		$301,675,000		$276,675,000		$256,075,000
Net Losses & Loss Expense Paid During Calendar Year	**$43,664,000**	**-5.32%**	$46,119,000	-8.22%	$50,247,000	31.83%	$38,116,000
Cumulative Since Inception	**$949,664,000**		$906,000,000		$859,881,000		$809,635,000
Reserve for Unpaid Losses & Loss Expense**	**$125,126,000**	**-3.60%**	$129,804,000	1.76%	$127,556,000	-4.65%	$133,781,000

Statements of financial condition, policyholders surplus, underwriting expenses, and operations, audited by Ernst & Young LLP, will be provided to policyholders upon request.

but it's nice to enjoy them when they come around.

Internal operations

The internal operations of MIEC continue to receive high marks from our customers. We constantly seek to improve our capabilities and operational efficiencies, and this is why our overhead is consistently lower than most of our (larger) competitors. Relative to other insurers, we allocate a disproportionate amount of resources to the areas of most value to our insureds - loss prevention and claims services.

This allocation is likely to continue into the future as we firmly believe that the best way to control malpractice costs is to:

1) fight non-meritorious claims and
2) help policyholders prevent claims from being filed in the first place.

In 2011 we continued to invest in staff and in our analytic capabilities to collate meaningful data that we believe will help policyholders improve patient safety measures (and so reduce claims for malpractice) in their practice. Specifically, MIEC has entered into a relationship with CRICO – a group of companies formed by the Harvard Medical Institution in the 1970's to handle its self-insurance program. Our partnership with CRICO will enable us to clinically code our open and closed claims so that we can identify causes of malpractice claims in our own portfolio as well as having access to the huge and widening database and patient safety intelligence that CRICO has accumulated over the past 30 years.

Not all claims can be prevented, so, if you do experience a claim, MIEC continues to provide the highest quality claims handling with our outstanding claims staff and defense counsel panel. The teamwork between MIEC staff and outside counsel makes a huge impact on the cost and quality of our defense. These individuals have often worked together on hundreds of cases over the past 3 decades and have produced consistently excellent results. In 2011 we closed over 90% of our policyholders' claims without payment to the plaintiff, a level of success that has persisted at or around the same level for many years. See ***Figure 2***.

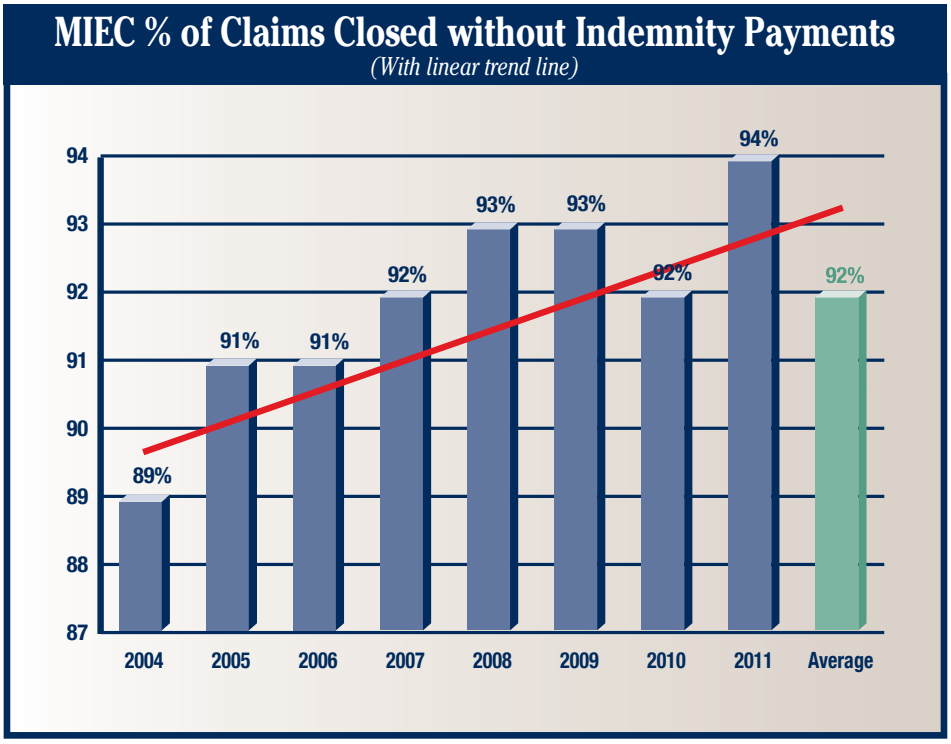

Figure 2

Inevitably, there are cases where there is liability and we take a proactive approach to reaching a fair resolution as quickly as possible. We believe this is in the best interest of our policyholders and also for injured patients. We also continue to believe that, in cases where there is no liability, our policyholders should be defended - through trial if necessary. During 2011 we tried 13 cases, winning 11 (and 1 hung jury) which is consistent with our 20 year success rate of 84%.

Overall, the claim results in the 2011

calendar year were among the best in our history and were a major driver of the dividends that policyholders received at this recent renewal.

Policy enhancement

An important new cover has been added to the MIEC policy in 2012. In recent years new laws and regulations have introduced explicit responsibilities in many areas, including medicine, to protect private information and established onerous duties on what must be done if protected information is compromised. MIEC has introduced a new policy endorsement (DataGuard) that automatically provides all policyholders with a basic level of coverage to help address the costs our policyholders might face when investigating and addressing a possible breach of confidential information. Additional limits may be available subject to additional underwriting. We urge our policyholders to visit our web site to learn more about how to protect themselves from this new area of liability **http://www.miec.com/WHOWHEREWEINSURE/DataGuard.aspx** (Note: You will need to log in to access these materials.)

Communication enhancement

MIEC is proud to report that we have extended support to our sponsoring medical societies by underwriting a valuable new communication "app" for android and iphone / ipad called DocBookMD. We have always encouraged MIEC policyholders to be engaged with and support organized medicine through membership in the state and county medical societies in your area. DocBookMD is a valuable free benefit that is only available through medical society membership.

Retirements

2011 saw the retirement of two people who have made a significant and enduring contribution to MIEC.

Dr. Russell Stodd of Kahalui, Hawaii retired from the Board this past December. Russ practiced Ophthalmology for over 3 decades and served the MIEC board in various capacities for 12 years. His successor from Hawaii is Dr. Gary Okamoto.

Bill Guertin was for many years the Executive Director of the Alameda Contra Costa Medical Association and was Chairman of the Board for MUC – the service company which administers all of MIEC operations. Bill has been a part of MIEC since its infancy and was a tireless advocate of physicians' interests for 40 years. He is succeeded by Don Waters.

During 2011, MIEC and its subsidiaries were subject to no less than 6 routine audits by a combination of accounting firms and state/ federal authorities. All of the audits reported a "clean bill of health" which is a testament to all those who serve on the Board of Governors and approximately 65 extraordinary staff who are proud to work on your behalf.

While the practice of medicine is under enormous stress, MIEC policyholders can be assured that their professional liability insurance is in excellent condition and that the organization is focused on serving the best interests of its policyholders. In each of the past 3 years we have lost less than 1% of our policyholders to competitors – a retention ratio that is the envy of any insurance company. This suggests to us that we are doing something right, but in no way makes us complacent.

We thank you for your support and loyalty. MIEC remains committed to a true not- for- profit conviction while also continuing to improve our service and capabilities so that we can serve you throughout your career.

MIEC's Business Philosophy

- Doctors first
- Clear, unambiguous and transparent rates set at a level to break even (i.e., we do not attempt to profit from operations)
- Low overheads – among the lowest in the industry
- Quality risk selection and careful underwriting
- Professional and uncompromising claims defense
- Thoughtful and practical Loss Prevention programs which are provided free to policyholders
- Collaborative relationships with organized medicine / medical societies
- Conservative investment philosophy with emphasis on investment income to further offset overheads
- Resilient balance sheet to insulate policyholders from unrelated events causing changes in the cost of MPL insurance
- Long-term approach to business initiatives
- Alignment of our operations and services to match those of our policyholders

Feature article – Hospitalist communication: risks and strategies

Case study

A 43 year old married father of three was taken via ambulance to the ED with sudden onset of mid-sternal chest pain as well as numbness and pain radiating to his left arm. History obtained by paramedics included shortness of breath, diaphoresis, abnormal EKG and five similar episodes in the last two weeks. The patient's serial cardiac enzymes, admitting EKG and chest x-ray were normal. The patient was admitted by Hospitalist A to the Telemetry Unit to rule out MI. The next day, the patient was feeling better and Hospitalist A ordered an exercise stress echo and noted "cardiology to see."

The stress echo was read by a cardiologist as showing no myocardial eschemia, frequent PVCs in recovery and excellent exercise tolerance; impression: normal. The cardiologist did not examine the patient, and it is disputed as to whether he was asked to perform a consultation or merely to interpret the stress echo, as there was no medical record documentation specifying the cardiologist's role in the patient's treatment. (Expert reviewers opined in retrospect that the stress echo was not normal.)

On the third day of hospitalization, Hospitalist B was contacted by a nurse who reported the patient's oxygen saturation was 90% on room air; a spirometry test was ordered and revealed severe obstruction and low vital capacity. Hospitalist B spoke with a cardiology physician assistant (PA) and requested a consultation and results of the echocardiogram. Again, the specifics of the conversation were not documented in the patient's chart, and it was disputed at trial as to whether a consultation was requested or merely a reporting of the test results.

Based on the normal echo results the cardiology PA discharged the patient with instructions to follow up with his PCP and continue Zantac and Lopressor. In her discharge summary, Hospitalist B did not

address the spirometry results, nor did she specify a plan for follow-up.

The patient saw his PCP two days after discharge and reported his recent hospitalization and negative cardiac studies. A spine film was ordered to rule out cervical radiculopathy and he was given a GI referral. On the next day, the patient called his doctor after experiencing three episodes of chest pain. He was advised to follow up with his GI consult. Nine days post discharge (before his appointment with gastroenterologist) the patient experienced chest pain and called an ambulance, but expired en route to the hospital. Autopsy showed "critical coronary artery stenosis."

Claims of medical negligence were made against Hospitalist A, Hospitalist B, the cardiologist, the cardiology group, the cardiology PA, and the primary care physician. The case was settled on behalf of the cardiologist and cardiology group in the mid six-figure range and the case was settled on behalf of Hospitalist B in the low six figure range. Hospitalist A and the primary care physician were dismissed.

This case illustrates how poor understanding of the division of responsibilities between the hospitalist and the cardiologist and poor communication between the hospitalists, cardiologist, and primary care physician resulted in the arguably unnecessary death of the patient. Essentially, no one took responsibility for the patient. It also illustrates that a lack of documentation of the treatment plan and disputed recollections hindered the defensibility of all of the defendant physicians. Although the bulk of the responsibility fell to the cardiologist, whom expert reviewers determined misinterpreted the stress echo, expert reviewers opined that Hospitalist B relied too strongly on the "normal" echo in determining that the patient was ready for discharge and failed in her duty to adequately address the spirometry results.

Mnemonics and standardized hand-offs

Handoffs occur any time there is a transfer of responsibility for a patient from one caregiver to another. As we can see from the case example, it is vital to patient safety to establish role clarity amongst the treatment team members and goal clarity in the treatment plan.

Regulatory bodies are well aware of the dangers of ineffective hand-offs. Problems with handoff communication are listed as one of the root causes in up to 70% of adverse sentinel events compiled by The Joint Commission, and hospitals seeking accreditation are required to have a standardized method for hand-offs. According to several hospitalist groups surveyed by MIEC's Loss Prevention field staff, it is often routine for hospitalists to facilitate the hand-off via a telephone reporting system. The clinicians record a message for their colleagues summarizing a patient's status. Unfortunately, the recorded message usually is not retained or memorialized in the chart by either the transferring or receiving hospitalist.

Hospitalists can better protect themselves, their colleagues and their patients by documenting receipt of the message. Example language might be, "Reviewed chart, MAR, shift report from Dr. XX [hospitalist]; discussed case with cardiologist Dr. XX, and family. No significant changes since yesterday." If there has been a significant change with the patient (positive or negative), the physicians should document the new information and any conversation between the two physicians.

Several mnemonic tools have been developed to assist members of the health

care team in accomplishing thorough, standardized hand-offs, including the FIVE-Ps (Patient, Plan, Purpose, Problems, Precautions), SBAR, I PASS the BATON, and more. For example, I PASS the BATON, which was developed by the Department of Defense's Patient Safety Program, was designed to work in conjunction with opportunities to ask questions and clarify information.

There is scant data available demonstrating the superiority of one standardized hand-off system versus another; the unique needs of each health care organization will likely determine which system is optimal. Regardless of which system you use, document the evaluation in the daily progress note. Electronically generate the notes (e.g., EMR, dictation/transcription) as these types of notes have proven to be more detailed than handwritten chart entries. It is also necessary to identify and correct systemic issues that prevent effective hand-offs, such as noise, interruptions, and unavailability of pertinent or pending test results and other data.

Communication with primary care physicians

In the case study, the patient's primary care physician was falsely reassured by the patient's recounting of the negative cardiac studies and did not consider MI when the patient called with additional complaints of chest pain. Had the primary care physician been aware of the spirometry results, might he have been more cautious about the patient's reported symptoms? Primary care physicians are often hamstrung by a lack of information about their patient's hospitalizations. Consider the following:

I	Introduction	Individuals involved in the handoff identify themselves, their roles and jobs
P	Patient	Name, identifiers, age, sex, location
A	Assessment	Present chief complaint, vital signs, symptoms and diagnosis
S	Situation	Current status and circumstances, including code status, level of certainty or uncertainty, recent changes and response to treatment
S	Safety Concerns	Critical lab values and reports, socioeconomic factors, allergies and alerts, such as risk for falls
the		
B	Background	Comorbidities, previous episodes, current medications and family history
A	Actions	Detail what actions were taken or are required and provide a brief rationale for those actions
T	Timing	Level of urgency and explicit timing, prioritization of actions
O	Ownership	Who is responsible (nurse/doctor/team), including patient and family responsibilities?
N	Next	What will happen next? Any anticipated changes? What is the plan? Any contingency plans?

- Researchers from Mt. Sinai School of Medicine in New York found that more than one-third of recommended outpatient work-ups following a patient's hospitalization were not completed because the discharge summary didn't include details of the work-up, or the summary wasn't available to the primary doctor at the time of the patient's follow-up visit.

- A study published in the September 2009 edition of the *Journal of General Internal Medicine* found that while all patients in the study were waiting for test results at the time they left the hospital, only a quarter of discharge summaries mentioned any pending tests, and a scant 13% documented what those pending tests were.

  Effective discharge handoffs are receiving more attention and resources thanks to public reporting of readmission rates and decreased reimbursement for readmission within 30 days. The Society for Hospital Medicine (SHM) has developed its BOOST program and is conducting pilot projects in several states. The BOOST toolkit is available on the SHM web site (www.hospitalmedicine.org). In addition to discharge transitions, hospitalists must have effective communication channels with primary care physicians to address patients directly admitted by those PCPs. Both hospitalists and primary care physicians share the responsibility of ensuring adequate hand-off communication at admission and discharge. MIEC recommends:

- Speak with each other. Do not assume that the primary care physician received pertinent records regarding admissions;
- Review all pertinent tests and results, which specialists saw the patient, and what the follow-up plans are;
- Convey any lab or diagnostic results that were outstanding at discharge and clearly designate responsibility for following up on outstanding results;
- Ensure that it is hospital policy to forward discharge summaries to the PCP of record; and
- E-mail or fax a thorough, timely discharge summary.

Scheduling and group organizational techniques

Traditionally, many hospitalist groups determine workflow and scheduling policies based on attempts to create equal work hours on a day-to-day basis. However, many groups are looking at innovative scheduling and assignment structures that aim to enhance communication, decrease disruptions, and enhance rapport with patients and primary care physicians. Would any of these strategies work for your group?

- Assign each hospitalist to designated primary care physicians (Hospitalist A always sees patients of Dr. Smith and Dr. Jones; Hospitalist B always sees patients of Dr. Johnson and Dr. Brown, etc.). This enables the hospitalist and primary care physician to get to know each other and to develop effective communication channels. Patients will likely welcome seeing a familiar face when admitted to the hospital.
- Do not assign new patients to a hospitalist the day before he or she is rotating off. Upon instituting this policy, one hospitalist group found that 71% of patients saw the same hospitalist throughout their stay, versus 57% under the previous policy which allowed assignment on the day before rotating off. This strategy also provides physicians rotating off with more time to have thorough discussions with patients, families and co-treaters, and to write notes.
- Have separate admitters and rounders, so that rounders don't have to drop what they're doing to go to the ED to admit or rely on holding orders that they can't be sure are appropriate

without evaluating the patient. Your colleagues in the ED may benefit from this approach as well, and once again patient satisfaction may increase through timelier admission.

- Enlist the patient and patient's family members as much as possible in hand-off processes. Educated, engaged patients can be terrific advocates for their own safety. Conduct hand-offs at bedside, involving the patient and the patient's family. Clearly document patient and family understanding of the discussion.
- Conduct patient-centered, multi-disciplinary rounds, including any staff member or provider involved in the patient's care (e.g., attending, resident, respiratory therapist, physical therapist, occupational therapist, social worker, pharmacist, charge nurse, individual patient's nurse, and pastoral care provider). Focus on collaborative decision-making and goal clarity.
- To the extent possible, assign patients to wards geographically, similar to the ICU, to reduce time wasted in transit between patients located on several different floors.

Hospitalists face many challenges in ensuring safe transitions in care; some hurdles may only be addressed if hospitalists take a leadership role and work closely with PCPs, nurses, administration, the emergency department, specialists, and even the IT department to remove barriers to safe, effective hand-offs.

Resources:

"Avoiding Malpractice Risks in the Patient Handoff," by Mark E. Crane for Medscape Business of Medicine, posted 05/10/2010

"Patient Handoffs," by Lee Ann Runy, Hospitals and Health Networks Magazine, May 2008

Society of Hospital Medicine 2010 Annual Meeting

From the Claims Department

Claims Q & A Corner

(California policyholders) I just received a letter from the Medical Board of California (MBC) requesting a copy of my medical records, CV, and a description of care of one of my patients. Should I respond immediately, or first seek advice?

If you receive any correspondence from the Medical Board, DO NOT respond without first contacting the MIEC Claims Department. Here is why…

All complaints and reports of settlement received by the MBC are first evaluated by the Central Complaint Unit (CCU). In response, the CCU sends the physician a letter requesting the records, a written response, and a CV. Each matter, including the records and narrative description, is reviewed by an analyst and a physician expert in your medical specialty.

Based on the initial review, a determination will be made whether to refer your matter from the CCU to the regional district office for further investigation. At the regional district level, your file will be transferred to one of the district's Medical Board investigators, all of whom are sworn peace officers. A personal interview will be requested, and your interview will be tape recorded. Furthermore, your interview will be attended by both the investigator and a district medical consultant, who is a board-certified physician who may or may not practice in the same specialty as you.

Based on the regional district review, your matter may be further referred for review by a panel medical expert in your specialty. Based on this tertiary medical review, your matter may then be referred to the Deputy Attorney General for possible filing of an Accusation, which is a formal legal action resulting in discipline and/or the suspension or revocation of your medical license.

In 2009, out of roughly 100,000 physicians practicing in California, the MBC CCU received approximately 6,500 complaints and other reports. Of those, about 5,200 were closed and 1,300 were referred to a regional district office. The relatively few matters that are referred on from the CCU are closely evaluated; therefore, it is in your best interests for the MBC to close your matter at the CCU level, rather than referring it on for further review. The best way to accomplish this is with the assistance of an experienced attorney.

Under Part II.B coverage, MIEC provides limited defense-only coverage for administrative proceedings in the amount of $25,000.00 for all incidents or investigations reported per policy year. Under this coverage, MIEC will retain a defense attorney with experience in defending Medical Board matters to consult with you and review your response to the Medical Board, in an attempt to have the matter closed at the CCU level. Your attorney will continue to represent you during the pendency of the Medical Board's investigation, up to and including a licensure hearing.

Please note: Narrative responses that are overly defensive, that discuss issues unrelated to treatment, or that attempt to deflect responsibility for an adverse event are viewed skeptically by the MBC, and are often referred to the regional district office for further review. Defense counsel can assist you in preparing a narrative summary that is respectful, factual, and that directly responds to the nature of the complaint or concern.

(California policyholders) What type of reports does the Medical Board of California receive?

First and foremost, the MBC receives complaints submitted by the general public; these are typically, but not always, from patients. Additionally, the Medical Board receives mandatory reports of settlement of professional liability claims at or above $30,000, as well as secondary reports from the National Practitioner Data Bank for any settlements or judgments below $30,000. All such matters are investigated through the CCU, including review of the records by a physician consultant.

The MBC also receives mandatory reports of administrative actions taken against physicians as a result of peer review. An example of this would be the suspension or revocation of hospital privileges. Such matters are referred directly to the regional district office without independent review by the CCU.

(California policyholders) I responded to the Medical Board several months ago but have not received any further correspondence. Should I contact them for a status update?

We understand that, after working to respond carefully and promptly to the MBC, you may be frustrated and concerned by the amount of time that may go by before receiving an update from them. However, it is best not to contact the Medical Board for updates on your pending investigation.

The Medical Board is required to investigate and respond to all matters in a timely manner, and matters that are closed by the CCU are often resolved within a couple of months after receipt of the physician's response. However, recent budgetary constraints have resulted in staff layoffs, furloughs, and an increased individual caseload that prevents the analysts and investigators from closely attending to all files.

Therefore, we recommend that you and your attorney avoid contacting the Medical Board for a status update and inadvertently attracting increased attention to your file.

Q (California policyholders) I have a notice from the Better Business Bureau (BBB) about a complaint from a patient of mine. What should I do?

A According to MIEC defense counsel, if a health care practitioner is notified by the Better Business Bureau (or Yelp or other consumer rating service) that a complaint has been made against him or her and the BBB wants the practitioner to respond, the practitioner should notify the BBB that he/she cannot respond until and unless the patient has signed an authorization for the release of patient information. Yes, this is true even though the patient has put the complaint process into motion and has put his or her care "at issue." Because the BBB is not a judicial or administrative forum (such as the Superior Court, Small Claims Court or the licensing board), there is no legal authorization for the practitioner to disclose patient information without the written consent of the patient. I acknowledge that it may be difficult for the BBB or the practitioner to secure the consent of an aggrieved patient, but it is essential that the practitioner err on the side of complying with HIPAA and state confidentiality laws.

Legal counsel confirmed with the Office of Civil Rights that authorization should be obtained before making a substantive response to a patient complaint. Also, a Supervisor at the Golden Gate BBB informed the attorney that many health care institutions require that patient authorization be obtained before they respond to patient complaints. Of note, the BBB is not supposed to accept medical malpractice or legal malpractice complaints, but often times billing complaints are tied up with medical care issues that can result in a practitioner disclosing confidential information; under HIPAA, even the fact a person is a patient is considered PHI, according to the OCR.

Feature article: Smartphones and HIPAA and texting…Oh my!

Text messaging or SMS (short message service) is a popular method of communication that has become part of everyday life. According to the International Association for the Wireless Telecommunications Industry (CTIA), 322.8 million wireless subscribers exchanged 2.12 trillion text messages in 2011. Like consumers, health care institutions and providers are incorporating text messaging ("texting") into their communication activities with noted improvement in the delivery of health care information, patient compliance, and the provider-patient relationship.[1] The ability to connect with a wide range of patients from pediatrics to geriatrics may prove beneficial in improving patients' outcomes;[2] however, caution must be exercised as privacy breaches, security risks, communication breakdowns, and increased liability exposure are potential consequences associated with medical text messaging.

Federal, state, local, and private institutions across the country have conducted studies to ascertain the effectiveness of medical text messaging.[3] The shared conclusion: with proper planning and an effective text message policy, texting is a medium that effects positive behavioral changes that improve patient compliance, patient education, disease management, and physician-patient communication.

Before texting medical information, physicians should determine the goal of using text messages and develop policies and procedures that define if and how they

1 **US Department of Health and Human Services** http://www.hhs.gov/news/press/2011pres/09/20110919a.html
Text4Baby http://www.text4baby.org/index.php/news/180-sdpressrelease
The American College of Emergency Physicians http://www.acep.org/Content.aspx?id=83825&terms=text%20messages
Denver Colorado community health centers http://www.ajmc.com/articles/Care-by-Cell-Phone-Text-Messaging-for-Chronic- Disease-Management
PricewaterhouseCoopers http://download.pwc.com/ie/pubs/2010_healthcare_unwired_new_business_models_delivering_care_anywhere_nov.pdf

2 Ibid

3 Ibid

and their staff will use texting. Policies should address prohibitions or guidelines for texting with patients and prohibitions or guidelines for texting with medical team colleagues. Some appropriate uses for texting with patients may include:

- As a compliance-improvement tool:
  - medication reminders
  - appointment or diagnostic testing reminders
  - reporting results of self-administered tracking devices
  - vaccination and immunization updates
- As an educational tool:
  - to dispense general and disease-specific health tips
  - public health information alerts, and discharge or aftercare instructions
- As a driver of patient satisfaction:
  - office wait-time updates
  - negative diagnostic test results
  - patient satisfaction surveys
  - birthday and other congratulatory wishes

Although these kinds of text messages with patients may be beneficial, there are risks to be aware of, including breaches of confidentiality; failure to transfer important clinical information to the patient's permanent medical record; "e-discovery" issues; and the potential for time-sensitive information to go unnoticed. If physicians decide that the benefits of texting outweigh the risks, we recommend that written text message policies be provided to patients and colleagues, as appropriate **(see Figure 3)**. It is essential to obtain patient authorization to communicate via text messaging, and doing so need not be burdensome. The perfect time to obtain patient authorization to communicate via text is during the registration process for new patients, and upon completion of the policy for existing patients. Copies of the policy should be placed throughout the office, and on the practice website.

Please note that even if patients authorize communication via text messaging, physicians are still beholden to state and federal confidentiality laws; if confidentiality is breached due to use of a text message, physicians must undergo confidentiality breach risk assessments and reporting requirements, regardless of the fact that the patient was apprised of the potential security risks of communicating via text message and elected to do so anyway.

Indeed, one of the biggest obstacles with texting health care information is the potential of a HIPAA or TCPA (Telephone Communication Protection Act) violation. State and local laws may also circumscribe texting activities. Most smartphones do not have data encryption built into the hardware, in which case a third-party application must be installed in order to encrypt the data. At the time of this writing, several Apple and Blackberry products have limited data protection, while Android smartphones do not have data protection. Physicians who opt to text patient-specific information to patients or colleagues would be wise to pursue the most secure options available.

Texting among medical colleagues

Texting should not be used as a substitute for a telephone call when discussing clinically significant, patient-specific information. A telephone call allows for two-way communication in which questions can be asked, information clarified, and mutual understanding verified. Texting of critical or emergent conditions can lead to patient injury unless there is some mechanism in place to ensure that

the recipient of such a text would receive it in a timely fashion and have the ability to speak with the sender of the text.

The standard of care associated with texting medical orders has come to the attention of The Joint Commission, which recently issued the following statement: "It is not acceptable for physicians or licensed independent practitioners to text orders for patients to the hospital or other healthcare setting. This method provides no ability to verify the identity of the person sending the text and there is no way to keep the original message as validation of what is entered into the medical record." This statement is not intended to be a blanket statement for using text messaging in a health care setting; rather, it is an attempt to ensure that physicians continue to orally communicate and sign their orders.

Documentation and e-discovery

Clinically significant patient information shared via text should be transcribed to the patient's medical record. Text messages may not be permanently stored and available in the event of a lawsuit brought months or even years after treatment, and the details stored in such a text message could make all the difference in your defense. On the other hand, the discoverability of text messages should encourage physicians to resist making subjective remarks that may be potentially harmful in the defense of a malpractice allegation. Do not text anything in conjunction with patient information that you would not want read aloud in a courtroom.

Using text messaging in your practice

Regardless of your goals, a carefully constructed texting policy and strict adherence to it will reduce your liability exposure. MIEC offers the following recommendations for using text messaging in your practice:

1. **Be cautious:** Protected Health Information (PHI) and Personal Identification Information (PII) are easily compromised. Most text messages are not secure or protected. Unless your mobile phone provider includes encryption software, the contents of your text message may be intercepted by an unauthorized party. In addition, text messages may be considered as, and pursued under, electronic discovery (e-discovery) in a medical malpractice allegation.
    a. Password-protect your smartphone so a password is required when accessed or in sleep/idle mode.
    b. Install "auto-lock" function to lock the device when not in use that requires a password to unlock.
    c. Install remote wiping device that erases data from a remote location when a Smartphone is lost or stolen.
    d. Obtain encryption to make it difficult for unintended recipients to read the text.
    e. End-user privacy is not guaranteed. Text messages may be opened in a public place where anyone near the receiver can view the message.
    f. Include texting as part of your HIPAA Risk Analysis.
2. **Be clear:** As with any encounter where face-to-face communication is substituted, the absence of oral, visual, and auditory cues may compromise effective communication.
    a. Develop a Digital Communication Policy **(see Figure 3)** that includes all methods of digital communi-

cation (e.g., text messages, e-mails, instant messages, social networks, blogs and online chats) and specifically states under what circumstances digital communication can be used to exchange medical information with patients, colleagues, and staff through a smartphone, laptop, desktop, notebook, or other devices.

i. Keep tone professional. Limit the use of abbreviations or "text-lingo." Contents may be easily misinterpreted if unknown abbreviations are used.

ii. Determine the extent of texting. Will it allow "two-way" texts allowing the receiver to respond or "send only" preventing the receiver from responding?

iii. Insist that patient "Confirmed opt-in" to ensure validity of telephone number.

iv. Include "opt-out" or "Stop" option with text message.

v. Double check telephone number for accuracy before sending.

3. **Be diligent:** Smartphone stored data may be compromised in the event of device failure. Although short, text messages that contain clinical information should be treated and documented like a telephone call in which medical information is relayed or requested and included as a permanent part of the medical record.

a. Texts should be printed, dated, signed, and filed into the patient's chart. A designated paper or electronic "digital communication folder" can serve as a repository for digital communication for which an electronic chart is not available (e.g., digital consult).

For Our Patients
Information about Text Message Communication and Our Text Message Policy

You have asked to communicate with our office via Text Message. To do so with safety and confidence, you must understand and agree to our guidelines. Please read the following information about Text Message communication and our Text Message policy. If you have any questions about what you read, please ask us or a member of our staff.

Following this information is an agreement that will protect your well-being and your confidentiality. If you understand our Text Message policy and agree to adhere to it, please sign and date the form. We will give you a copy to take home. If, at any time, you wish to discontinue Text Message communication with this office, please submit your request in writing to us or a member of our staff. Thank you for your cooperation.

- Please be aware that Text Message communication is not a substitute for a face-to-face encounter with a physician.
- It is our practice to make every effort to protect your confidential information in all communication. (Optional: List protection technology such as firewall, secure network, encryption, automatic logout, password protection, need-to-know access, etc.) We acknowledge, however, that no Text Message is 100% secure. Even the most carefully protected messages are stored on a smartphone. Though it is unlikely, this information could be retrievable. We cannot guarantee against unknown privacy violations such as unauthorized access achieved by illegal activity.
- We ask you to limit your Text Message communication with us: to ask routine, non-urgent medical questions; to schedule an appointment; or to report a mild reaction to treatment.
- We will communicate with you via Text Message only if you are an established patient. That means that we will communicate with one another only in the context of care that began with a face-to-face encounter.
- All Text Message communication will be printed out and a hard copy will be filed in your medical chart.
- We will try to respond to Text Message messages within XX hours. However, there is no way to guarantee that this will occur, for a variety of legitimate reasons. (Optional/examples: misaddressed Text Message, connection problems, etc.) If you do not get a response from this office within XX hours, it is up to you to contact us by telephone, mail, fax, or in person.
- We do not accept medication refill requests by Text Message unless the request was preceded by a recent exam in the office. Even then, good medical practice may mean that it is necessary for you to be seen before we can refill your medication.
- We will do our best to avoid technical problems. However, if a malicious virus infiltrates our system, we cannot guarantee that we could prevent it from inadvertently passing to your smartphone.
- If we are out of the office or if we are with other patients, a medical assistant will print out Text Message messages for us and, at our direction, may respond to you on our behalf.
- If you fail to adhere to our Text Message policy, we will discontinue our communication with you via Text Message.

Please alert us to any questions you have about what you have read.

Figure 3, page 1

Our Agreement

I wish to communicate with the office of Dr. XX and Dr. XX by Text Message. I am aware that Text Message communication is not 100% reliable or secure, but I acknowledge that the doctors and their staff assured me that they make every effort to protect my privacy. I wish to use Text Message to communicate with them.

1. I am aware and agree that a hard copy of all Text Message correspondence will be filed in my chart.
2. I will limit my Text Message to: ask routine, non-urgent medical questions; make an appointment; request a non-narcotic prescription refill; or report a mild reaction to treatment.
3. **I** agree to fill in the subject line of each Text Message to alert the doctors and their staff of the purpose of my message. (e.g., REFILL; QUESTION; APPOINTMENT; etc.)
4. I will not Text Message my doctor regarding emergencies, as I am aware that time-sensitive matters are not appropriate for Text Message communication.
5. I will not communicate by Text Message about information or questions related to 1) highly sensitive subjects such as HIV/AIDS or STDs; 2) questions or problems of a sexual nature; 3) alcohol or drug dependence or treatment; or 4) questions about my mental health.
6. If I do not get a response to my Text Message within XX hours, I will contact the doctors or their staff via other means.
7. I know I am responsible for following the medical advice the doctors convey to me by Text Message.
8. I accept that if I fail to follow this agreement related to our Text Message correspondence, that the doctors will limit my correspondence to more traditional means, such as the telephone and/or US mail.
9. I request and authorize the doctors or their staff to communicate my routine negative lab results to me via Text Message.

11. I have asked all the questions I had about the practice's Text Message policies and my questions were answered to my satisfaction. I understand the policies and agree to abide by them in full.
12. (Optional: I agree to pay the practice's fees for Text Message communication in the event my health insurance or mobile carrier do not cover the charges.)

_____ _____

Patient's signature Date

_____ _____

Patient's Text Message number Home number

_____ _____

Doctor's signature Date

☐ copy to patient

Figure 3, page 2

From Underwriting and sponsoring medical societies

Summary: *The passage of the HITECH Act reminds physicians who qualify as "covered entities" that state and federal privacy and security rules and regulations must be a priority for them. Yet studies demonstrate that, in spite of the ever growing number of physicians who are implementing electronic healthcare records, clinicians fail to adequately safeguard data and the devices which house it. To better protect policyholders who may find themselves faced with a data breach, physicians should consider cyber liability coverage as part of their malpractice policy.*

It's hard to believe that it has been over a decade since the HIPAA Privacy and Security Rules went into effect with mandatory compliance dates of April 14, 2003 and April 21, 2005, respectively. Physicians and their staff have labored to act in accordance with these cumbersome regulations by developing and implementing policies and procedures that shield protected health information (PHI); advising patients how their PHI may be used and their right to limit access to the data; identifying business associates, safeguarding the transmission of e-PHI, and much more.

The decade that brought healthcare providers the HIPAA regulations also witnessed massive expansion into the world of technology to transmit and store PHI and promote collegial communication. Electronic healthcare records, smartphones, email, communication portals, laptops, iPads, eICUs, telemedicine, social networks, and data storing "clouds," just to name a few. The capability for physicians to "connect, communicate and collaborate" electronically via the HIPAA-compliant smartphone platform DocBookMD is still another example of innovative healthcare technology. (For more information about access to this MIEC and medical society-sponsored professional network, visit your local medical society's website. See ***Figure 4***).

Although federal and state regulators encouraged the development and use of healthcare technology, they again raised the bar of responsibility for physicians and their business associates with the passage of the HITECH breach notification regulation that went into effect on February 17, 2010. The HITECH Act reinforces the HIPAA Privacy and Security Rules, outlines a data breach notification process, and threatens significant fines for noncompliance.

In spite of the heightened awareness of both federal and state confidentiality rules and regulations, the 2011 Ponemon Institute "Second Annual Benchmark Study on Patient Privacy and Data Security,"

Introducing DocBookMD, a smartphone platform designed by physicians for physicians.
With DocBookMD, users have access to:

1. **On-Demand Messaging**
2. **Multi-Media Collaboration**
3. **Fast Look-Up of medical society colleagues**
4. **Quick Pharmacy Search**
5. **Use on Multiple Devices**

It's easy to get started: Download DocBookMD from the iTunes App Store or the Android Market. Open the app and begin the registration process. You may need your medical society ID number.

Figure 4

illustrates that healthcare data breaches are on the rise and more work needs to be done to protect PHI, computing devices, and patients harmed by data breaches:

- 96% of all healthcare providers who participated in the study had at least one data breach in the last two years;
- 49% of the respondents cited lost or stolen computing devices;
- 81% of the healthcare organizations in the study reported the use of mobile devices to collect, store, and/or transmit some form of PHI;
- 49% of the participants admit that their organizations do nothing to protect the devices;
- Only 29% of respondents agreed that prevention of unauthorized access to patient data and loss or theft of such data is a priority in their organization; and
- 90% of the surveyed healthcare organizations indicated that the breaches caused harm to patients; however, 65% did not offer protection services to the affected patients.

These statistics are disturbing; however, perhaps more disturbing are the reported costs to participants in the study. The average economic impact of a data breach was $2.2 million. While this data reflects the costs of larger organizations rather than the typical medical group, it is an indication of the expenses associated with recovering from a data breach. In addition, 81% of the 2011 Ponemon study respondents believe their organization suffered from time and productivity followed by brand or reputation diminishment (78%) and loss of patient goodwill (75%). The average lifetime value of one lost patient rose from $107,580 in 2010 to $113,400 in 2011.

MIEC is here to help policyholders be compliant with HIPAA

Revisit the HIPAA Privacy and Security Rules and learn more about the HITECH regulation by visiting MIEC's website at www.miec.com. The Loss Prevention Department has developed a number of supportive resources for you to download and adapt to your practice. Find helpful information on the website under the Resources by clicking on the HIPAA materials link in the sub-navigation (Note: most information requires policyholder login). Call our Loss Prevention representatives with any general HIPAA questions at our toll free number: 800-227-4527.

MIEC now protects its policyholders against privacy breaches with DataGuard coverage

As of February 1, 2012, MIEC provides the "DataGuard" endorsement to each physician's policy. With this new enhancement to the policy, you have peace of mind knowing there is basic insurance coverage to offset the costs that may be incurred to comply with regulations and for any lawsuits that may result from a breach.

DataGuard Coverage

Network Security & Privacy Insurance – Coverage for both online and offline information, virus attacks, denial of service, first-party HIPAA violation coverage and Red Flag Regulations. This includes coverage for fines and penalties from privacy regulatory actions.

Patient Notification Costs & Credit Monitoring Insurance – Coverage for necessary legal, PR, advertising IT forensic costs and postage expenses incurred by you to notify third persons of a breach of information. Will also pay for one year of credit monitoring for all affected parties.

Data Recovery Costs Insurance – Coverage for reasonable and necessary sums required to recover and/or replace data that is compromised, damaged, lost, erased or corrupted.

Figure 5

The DataGuard protection covers most of the types of expenses you may have to pay in the event of a privacy breach with a limit of $50,000. This is a basic level of protection. Given the expenses involved in responding to a breach, we strongly suggest policyholders consider higher limits of coverage by completing a very simple one page application available at www.miec.com. See ***Figure 5***.

MIEC also provides an electronic platform for information that will enable you to understand and deal with these new and evolving exposures. Explore these tools by visiting the website and logging in. Go to the "Who & Where We Insure" tab; click on the DataGuard link in the subnavigation. This includes unlimited online access to tools and resources that help mitigate a breach, such as:

- Compliance materials with state by state rules and regulations;
- Implementation checklists to help protect, detect, contact and correct any security violations;
- Training programs such as webinars, bulletins, online modules for you and your staff; and
- Step-by-step procedures to reduce risk including information on the proper destruction of protected health information.

Call MIEC's Claims Department if you experience (or believe you have experienced) a data breach! Don't delay! Implement the changes that you need to make to be in compliance with the HITECH Act. Call immediately for assistance.

MIEC is owned by the policyholders we protect. Let us protect you today!

MIEC joins the PDR Network to help policyholders reduce ADEs!

PDR® Network
Safety Communication Compliance

PDR Network is the leading distributor of drug labeling information, product safety Alerts, and Risk Evaluation and Mitigation Strategy (REMS) programs. These include Physicians' Desk Reference® (PDR®), PDR.net®, *mobile*PDR® and PDR Drug Alerts, the only service providing electronic delivery of mandated safety Alerts to physicians and other prescribers. PDR now incorporates a broad suite of services into physicians' electronic healthcare records (EHRs) including the adverse drug event reporting service **RxEvent.org**. Partners to the PDR Network include 30 medical specialty and state medical societies, MIEC and over 40 other liability carriers, and iHealth Alliance.

The iHealth Alliance is a PIAA-sponsored not-for-profit organization whose primary mission is to protect the interests of patients and healthcare providers as they adopt electronic systems to provide quality health care. The iHealth Alliance governs PDR Drug Alert delivery and oversees the development of independent CME associated with Drug labeling, Drug Alerts and REMS notifications, as well as overseeing PDR Secure™, PDR Network's Patient Safety Organization (PSO). For more information about the PDR Network, visit www.pdrnetwork.com.

iHealth Alliance and PDR Network partners create EHRevent.org.

iHealth Alliance

As the number of EHR systems increase and as they are integrated with other systems to import and exchange data, it is imperative for EHR users to track and understand issues of concern as they develop. Such knowledge will allow for improvement in EHR technology, patient safety, and will help physicians decrease their risk of liability. Together with professional liability carriers, iHealth Alliance created **EHRevent.org,** a safety event reporting system. Reported information is kept secure via the federally-certified Patient Safety Organization PDR Secure™. For more information, visit www.ehrevent.org.

How to reach MIEC

PHONE:

Oakland Office: 510/428-9411

Honolulu Office: 808/545-7231

Boise Office: 208/344-6378

Outside: 800/227-4527

FAX:

Main Oakland Fax: 510/654-4634

Honolulu Fax: 808/531-5224

Boise Fax: 208/344-7903

E-MAIL:

Lossprevention@miec.com

Underwriting@miec.com

Claims@miec.com