

President's Letter

Welcome to 2001 NC ASHRM! As your new President, I am honored to be serving the Chapter at a time when healthcare, and risk management in particular, faces the public and professional fall-out from the Institute of Medicine report on quality and safety in medical care. In addition, the new JCAHO patient safety standards take effect in July 2001. Assuring ongoing, focused attention to the protection of patients, employees, and medical staff will be an opportunity and a challenge for our profession in the coming year.



Richard Thompson

To meet these and other challenges, I will work through the board and membership of NC ASHRM to provide educational programs dealing with current issues in healthcare focused on clinical risk and quality issues, practical skills, and personal growth. In addition, we will continue the "Toolbox" sessions initiated at the Fall Meeting at Sunset Beach. The "Toolbox" sessions are open to all educational meeting participants, though they may be especially helpful to the new risk manager.

The 2001 Board has been hard at work since December 2000, when the outgoing 2000 Board met with the new 2001 members to assure a smooth transition. The 2001 Workplan builds on the "Back to Basics" theme of 2000 for the Chapter. Main points of emphasis for 2001 are:

- Enhance use of the Chapter Newsletter to communicate Chapter business and Board activities to the membership
- Continue active support of ASHRM
- Strengthen the link between NC ASHRM and appropriate NC legislative members and committees to better position NC ASHRM as a valued resource on matters of healthcare risk exposures
- Continue to encourage the professional and personal development of individual members through educational programs and resource identification
- Recognize the accomplishments of members and of the Chapter
- Encourage members to participate actively in the business of the Chapter
- Continue our Sponsorship program by providing value and recognition for the contributions made in support of our Chapter

Continued on page 7

MANAGING THE ELECTRONIC WORKPLACE: E-MAIL AND THE INTERNET

By James T. Harrison Jr., J.D., CIC, CPCU, CLU, ChFC

Reprinted with permission of the author

Agents and agencies have moved into the electronic workplace at a breakneck pace, with little concern for the potential legal and management issues this raises. In the workplace of today, automated systems and records are rapidly replacing manual procedures and paper documents, bringing the potential for escalating risks along for the ride. The "90's" were marked by a substantial increase in work-place technology and, at the same time, a greater sense of independence and autonomy in the attitude of the employee. The changing technology in this environment has produced new challenges for the agent as manager.

To understand the impact of the electronic workplace on agents as employers, agents must first understand the characteristics of the new technologies and the risks that these technologies pose. For instance, while e-mail can be used to transact business and increase efficiency, it can also be used to broadcast discriminatory remarks about other employees. Similarly, the Internet, as it opens doors to the vast resources of the information superhighway, may also open an employer's doors to employees' use of the Internet to access sexually explicit materials or to download copyrighted software. By understanding these new technologies, agents will be able to enjoy the benefits of the electronic workplace, while also minimizing the risk of litigation.

E-mail, Handy or Hazardous?

E-mail presents enormous benefits to agents and employees... E-mail encourages intracompany communication, increases productivity, and reduces the need for inefficient telephone

Continued on page 2

LETTER FROM THE PAST PRESIDENT: Chuck Mantooth

Sometimes it's easy to lose touch of who we are. Recently, I was browsing through some information received from National ASHRM and happened to come across the "American Society for Healthcare Risk Management 2000 Business and Strategic Plan." I was interested to see, in retrospect, how well the National chapter had succeeded in fulfilling the plan. My attention quickly focused on the overwhelming theme of the business plan; education, professional development and communication. The question came to mind of how well our organization performed in these areas. My answer was found by looking back at the chapter activities of this past year.



Many of you are aware that our focus in the year 2000 was to get "back to the basics". This meant for us to get "back to the basic." This meant for us to concentrate our efforts on providing forums for the exchange of information and ideas while encouraging professional development. We simply looked within our own membership to provide education, professional development assistance and communication ideas.

You may have noticed that our fall meeting include "risk management basics" which provided new and "seasoned" risk managers/health professionals the opportunity to share basic thoughts and ideas concerning risk management. You may remember the names of those who passed the CPHRM exam and an increasing effort on the part of other professional development committee to provide assistance to other members wishing to take this exam. You may also remember the final chapter newsletter from 2000 as being one of the best yet. You may not have realized it at the time, but all of these things were a direct result of increased focus on doing the things we do best, better.

Although there are numerous examples, these few things reaffirm my belief that this chapter is headed in the right direction. Although the leadership for 2001 has changed and members come and go, our theme remains the same. ♦

Editorial Comment

This, the latest issue of *AT RISK* is packed chock-full of information. Management of the Electronic Workplace, some thoughts from a modern legend, improving medication safety-these are all areas that risk managers need to be cognizant of. Hopefully this information will be of use to you in your daily work. I realize that we have a broad, diverse knowledge base in this chapter. We will attempt to tap into that knowledge throughout the year. Our goal is to provide high quality, interesting topics with an eye towards brevity. Please feel free to forward any comments, information, or articles to me.



— Sandra Butler

E-mail... Continued from page 1

calls, paper memos, and face-to-face meetings. However, e-mail can also have enormous potential for workplace mischief and can lead to dramatic developments in employment litigation.

Because of e-mail's informal nature and perceived impermanence, people often use e-mail to send messages that may be too candid to "put in writing," or inappropriate to make as a face-to-face statement. In addition, most e-mail systems create a complete record of the communication. The systems capture the exact text that users send and receive. Additionally, e-mail records usually store information regarding their transmission and receipt, including the names of the sender and the recipient, the dates and time that the messages were sent and received, and an acknowledgement that the e-mail was retrieved. This information may be of great value for clarifying which personnel were involved in making particular decisions, what officials knew, and when they knew it. The lesson is clear: unless backup files are regularly cleaned out, electronic communications remain stored indefinitely on a hard drive, backup tape, or disk, waiting to be found by the computer consultant hired by the attorney who was hired by a discharged and disgruntled former employee.

Courts are allowing the discovery of backup systems consisting of hundreds of thousands of tapes. This can be dangerous, because computer users often put messages into e-mail communications that they would never put into writing on real documents. Also, e-mail lasts longer than most users realize. Whenever an employee sends a message over the company's network, two or three copies of the message may be stored on file servers before being transferred to archive tapes. E-mail is more permanent than a paper communication. Paper documents can be shredded or discarded, but it is a far more difficult to destroy e-mail messages. Even after hitting the delete key, some e-mail systems store messages on a backup file for an indefinite period of time.

Agents should advise employees to use the same care in preparing e-mail messages that they would in drafting a letter on paper. E-mail often lasts longer than messages on paper and is easily forwarded to many other readers. Users of the e-mail system should be reminded that a promise made in an e-mail message is just as binding as one made in a letter, and that discriminatory or harassing comments are

improper in any form, whether verbally, written on paper, or posted in an e-mail message.

An employer's e-mail and voice mail policy should have a statement forbidding any messages containing offensive or sexual materials and should place an obligation on an employee to report such messages if received. The policy should state that e-mail and voice mail are to be used for business and professional reasons, not personal reasons. Such a statement may not prevent an employee from using e-mail and/or voice mail in a sexually hostile manner. However, the policy will be useful for discipline purposes and to defend against a claim of sexual harassment. Agents should emphasize in their policy that employees should not refer to or denigrate a person's race, color, religion, sex, age, national origin, disabilities, or physique.

The electronic workplace poses other hidden traps for agents. For instance, agents may be liable for an employee's uses of e-mail to send or received material that infringes a copyright, such as pirated software. Agents may also be liable for an employee's use of e-mail to send or receive trade secrets in violation of the rights of the owner of the trade secret, to publish defamatory statements, to send or received obscenity or child pornography, and for harassment. Additionally, an employer may be liable for an employee's use of e-mail to make statements or enter into contractual commitments that bind the company to a particular viewpoint, or to a contractual obligation.



Other Potential Perils

In addition, agents maybe subject to liability for the conduct of their employees in other ways. Employees who download unlicensed copies of software programs from the Internet or install pirated copies of application on their desktop computers leave their agents liable to legal challenges on copyright infringement. Software piracy is a common area of liability exposure on the Internet. If an employee uses company equipment to download software, and then wrongfully distributes the software or unlawfully makes changes to it, the company could be held liable for piracy-which is, in effect, copyright infringement.

A copy of a software program that cannot be validated by purchasing records might result in an allegation of copyright infringement. Agents should set guidelines for downloading software and data from on-line services and the Internet. Agents should also audit personal computers and network machines, and destroy any illegal software they find. Finally, agents are advised to keep a catalogue of all software licenses.

An employer may be liable for copyright infringement,

even if an employer did not actually perform the copying or distributing. Under the theory of contributory infringement, an employer may be liable for infringement committed by an employee if the employer had knowledge of the infringing activity, and induced or materially contributed to the infringing conduct. Under the theory of vicarious liability, an employer may be liable for an employee's infringement if the employer had the right and the ability to supervise the employee's activity, and a financial interest in exploitation of the copyrighted materials.

In this digital age, employees may be exposing their agent/employer to unprecedented liability risk now that many desktop computers in the workplace are interconnected to the Internet. For instance, pornography may enter the workplace as a result of an employee downloading graphic images from the Internet. Once these images are downloaded, they may be viewed on a computer screen or transmitted to other employees via e-mail. Under these circumstances, an employer may be exposed to a sexual harassment lawsuit or the employee, himself, may be engaged in criminal conduct.

One, largely unanticipated, problem with granting workers wide access to the Internet is the reality that when an employee visit is a Web site they leave a trail usually identifying the employer who owns the computer.

Undoubtedly, as a result of the use of interconnected computer systems, agents can be held liable for the acts of their employees in a variety of ways, including defamation (from inflammatory e-mail messages or harmful electronic bulletin board postings), copyright infringement (from installing or downloading pirated copies of software onto employer owned computers), sexual harassment (from offensive or hostile e-mail messages), obscenity (from downloading or distributing obscene graphic images or use of offensive material that is distributed by means of the workplace e-mail system), and discrimination. Finally, e-mail can be a very dangerous means of intentionally leaking corporate trade secrets. Loss associated with stolen trade secrets can be substantial.

Searching and Monitoring

One major concern in the electronic workplace involves efforts to search and retrieve voice mail, e-mail, and similar electronically stored messages. Agents often have a legitimate need to search an employee's e-mail or voice mail messages. The developing doctrine of employee privacy and the dramatic expansion of the electronic workplace have combined to create one of the most important areas of employment law as we enter the 21st Century. We have officially entered the information age where the amount of information that can be obtained about an employee is virtually unlimited. This rapid development of information technology and the mass availability of information have the potential to eclipse an employee's right to privacy in the workplace.

Indeed, another view of the impact of information technology on the workplace reveals that the unmistakably intrusive nature of digital technology and its many uses for workplace surveillance warrant an examination of whether an employee's privacy interest are sufficiently protected by current law. Not surprisingly, the formulation of the question may have a pivotal impact on the nature of the answer. In this respect, questions concerning the right of privacy often entail ready made assumptions about the importance of privacy; unfortunately, these assumptions limit or confine the privacy interest at the start of the analysis.

The various types of electronic monitoring currently in use include the following:

Telephone Call Accounting

Agents record such data as how many calls are made from a particular extension, which numbers are called, and the length of the calls. While this method is typically used to establish productivity quotas, agents have also used it to monitor the frequency and duration of personal calls. However, listening to the content of personal calls is illegal under existing legislation.

Telephone Service Observation

With this type of surveillance, supervisors listen to their subordinates' business telephone calls. Calls may be recorded for later listening, or supervisors may listen on line. This method is predominately used as a quality assurance check for employees who deal with the public.

Computer Monitoring

As alluded to earlier, software exists which allows managers to read their employee's computer screens. More common uses of computer monitoring, however, are counting keystrokes to measure speed of data entry, or monitoring time spent away from the computer.

The critical question raised by the power of electronic monitoring is how to balance an employee's right of privacy against the availability of tremendously valuable information. An employer must address this delicate balance and establish rules and regulations regarding its formation. The alternative is a dramatic increase in litigation costs. In fact, during the last decade we have seen an increases of 3,000 percent in the number of privacy lawsuits.

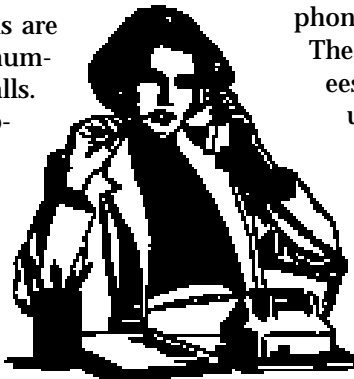
Although agents often have a legitimate need to conduct a search, cautious agents must be aware that their actions may violate an employee's right to privacy. If the employer has a legitimate need for the information and reasonably limits the scope of the search, the search will likely be regarded as protected and reasonable. One way to accomplish this goal is to notify employees that they and their

possessions may be subjected to searches at work.

In general, searches should be based on reasonable suspicion or legitimate business needs and limited in scope to that necessary to achieve their purpose. Further, agents should endeavor to reduce their employees' expectations of privacy. This can be accomplished in several ways. Written authorization could be obtained from the employees before the search. A well-designed employment addressing these issues is essential (an excellent sample of such a policy may be found at steveanderson.com).

The federal wiretapping law prohibits any person from intentionally intercepting, using, or disclosing any wire, oral, or electronic communication. In the employment context, this frequently arises in the context of an employer taping telephone calls made to and from the business phone. There are two exceptions relevant to agents.

The prior consent exception requires the employees' consent to wiretapping or monitoring must be unambiguous and clearly encompass the types of communications subject to the monitoring, although, apparently, it does not need to be explicit in writing. The business extension exception covers telephone equipment used for ordinary business purposes by the employer, such as switchboard systems, intercom equipment, as well as numerous phone extensions connected to the same telephone line.



A Watchful Eye

Generally, an employer may be able to monitor sales or marketing calls for training or other legitimate purposes. The exception, however, will not extend to the monitoring of personal calls made by the employees on the same telephone lines.

The business-extension exception allows the employer to monitor its employees when the device that intercepts a communication is a telephone or electronic communication system being used in the ordinary course of business. This exception allows for workplace telephone monitoring conducted by agents.

The ECPA (The Electronic Communications Privacy Act) clearly gives an employer the right to access an employee's e-mail and voice mail messages if the messages are maintained on a system provided by the employer. However, employers may not access messages if the system is provided by an outside entity, such as MCI mail, without the authorization of the employee who communicated the message or the intended receiver of the message.

Once the employer has accessed messages, it must be very careful about divulging their contents. The Act prohibits certain unauthorized knowing disclosures. The employer may disclose the message to the addressee or intended

recipient or to an agent of that person. The employer may also disclose the contents of the stored messages with the lawful consent of the originator or addressee of the message or the intended recipient of the message.

Thus, one method of limiting potential legal exposure is to conduct only “authorized searches and retrievals, and to limit the scope of search and retrieval efforts to that which is business related. Similarly, a well-established written policy regarding the employer’s ability to search and retrieve voice and a-mail messages also will assist agents in demonstrating that their conduct is “authorized.”

Agents should note that the ECPA also protects against the unauthorized access of electronic communications in electronic storage. E-mail in electronic storage includes e-mail that has been stored for backup protection. By definition, most e-mail exists in electronic storage. Therefore, any protection of employee privacy found in the ECPA will generally be based upon the unauthorized access provision.

The Omnibus Control and Safe Streets Act also regulates the interception of wire, electronic, and oral communications. The most significant exception to the Act provides that an employee may either expressly or impliedly consent to an otherwise impermissible monitoring of a communication. Accordingly, employers may avoid liability under the Safe Streets Act by procuring the consent of employees before monitoring communications. Agents should obtain express consent in writing.

Agents should be aware that state statutes and state common law may also limit the nature and scope of permissible searches. States that explicitly guarantee a right to privacy in their constitutions are Alaska, Arizona, California, Florida, Hawaii, Illinois, Louisiana, Montana, South Carolina, and Washington. In addition to statutory restrictions, courts in almost all state jurisdictions have long recognized various common law causes of action involving the intrusion into the personal privacy of individuals.

The single most important point for agents to remember regarding privacy in the electronic workplace is the need to reduce employees’ expectations of privacy in the workplace. To reduce

MEET OUR NEW MEMBERS



Sherry Cox
Risk Manager
Ashe Memorial Hospital, Inc
910-246-7101

Kristin Lehrer
Risk Manager
Carolinas Healthcare System
704-355-3238

Elizabeth Evans (Beth)
Quality Resource Nurse
Chowan Hospital
252-482-6378

Thomas Murphy
Vice President
The Reciprocal Group
804-965-1252

Dan Wright
Vice President
Risk Management
MAG Mutual Insurance Co.
800-282-4882

Lisa Kuney
Risk Management Coordinator
Onslow Memorial Hospital
910-577-2517

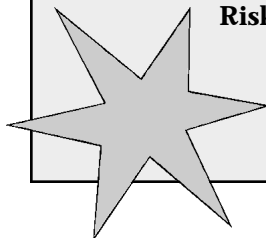
Anna Schofield
Risk Management Specialist
UNC Hospitals
919-966-0595

New Board Members 2001

Tom Eure
910-291-7509
tleure@carolina.net

Lisa Byrd
910-671-5586
byrd02@srmc.org

Congratulations to Jan F. Nair, Risk Management Analyst, Mission St. Joseph's Hospital, Asheville, NC, who has just completed the designation of Certified Professional in Healthcare Risk Management (CPHRM)



TIME AND TIDES

Lessons from Legends

(With Lifeguarding Vet Joe Pecoraro)

By Chris Serb

Reprinted from *Hospitals & Health Networks*, Vol. 73, No. 4, by permission, July 1999.
Copyright 1999, by Health Forum, Inc.

In 1949, 18-year-old Joe Pecoraro put on a lifeguard uniform for the first time - just for a couple summers, he thought, to help pay for college. Fifty years later, he's still pounding the sand. As head of Chicago's lifeguard service, he manages 1,000 guards, 30 miles of beach, and dozens of pools. During Pecoraro's 26 years at the helm, his lifeguards have made 150,000 rescues and lost fewer than 10 swimmers, a safety record unmatched anywhere. He recently shared some tips on consistency, teamwork, and crisis management with fellow lifeguard and H&HN staff writer Chris Serb.

Longevity

I couldn't have stayed for 50 years without keeping a balance. I don't work in the office or do paperwork the whole time. On weekends, I'm on the beach lifeguarding. If I couldn't hit the beach, I'd quit this job tomorrow. The action and the challenge just keep you going.

Crisis Management

When lifeguards make a rescue, they have only a split second to make a judgment and go into action. They have to rely on a couple of things: common sense, sound training, and a sixth sense they develop from experience. They can almost sense a rescue before it happens, even if none of the classic signs are there.

The business world works the same way. Lifeguards don't know what situations will happen, but they're always prepared to react. In business, you have to learn your industry well enough so that if something changes or a crisis happens, you can react. And not just make a quick decision - you have to use common sense and that sixth sense to make the right decision quickly.

Chain of C

President's Letter

Continued from page 1

All Chapter Committees have been assigned a board liaison; some Board members also serve as the Committee chairperson. If you are interested in serving on a Committee, please contact the chairperson or Board liaison - it's a great way to become more involved, learn more about the workings of your state and national professional associations, and contribute to your profession.

With the change in federal administration, the future of some healthcare regulations is not clear. However, it is clear that we could have great opportunities to improve both the working reality, and the perceptions of safety and quality in healthcare. I look forward to working with the 2001 Board, the Chapter Committees, and the membership as we face these challenges together. ♦

Richard Thompson
President

IMPROVING MEDICATION SAFETY

From the *AHA Quality Advisory*, December, 1999
Reprinted with permission from the American Hospital Association

Background

Most of what has been learned in recent years about how to reduce medication errors and increase patient safety is based on two principles. First, individuals, by the very nature of being human, are vulnerable to error. Although individuals are the focus of the error, errors happen because of the systems in which those individuals work. As a result, reducing error will require us to design and implement more error-resistant systems. Second, we have to create an environment in which we can learn from a failure safe, non-punitive environment that supports candid discussion of errors, their causes, and ways to prevent them.



These principles have a common denominator—they require the leadership and commitment of senior executives, medical, nursing, and clinical staff to create change within our organizations.

Common Sources of Error

Medication systems in hospitals are complex and multi-layered, involving many steps and many individuals. According to experts, this complexity increases the probability of failure. While many errors are caught before they can cause harm, it can be tragic whenever a patient's safety is compromised. Error can occur at any stage—prescribing, ordering, dispensing, administering or monitoring the effects of a medication. According to the Institute for Safe Medication Practices, some common sources of medication error in health systems include:

- **Unavailable Patient Information:** Critical patient information (diagnoses, lab values, allergies, drug contradictions, etc.) is often unavailable to pharmacy, nursing, and medical staff prior to dispensing or administering drugs.
- **Unavailable Drug Information:** Pharmacists often are not readily available on patient care units and written resources may not be up-to-date, which can lead to dose miscalculations or ignorance of drug interactions. Because errors occur most often during the prescribing and administration stages, accessible drug information must be readily available and close at hand for all staff who prescribe and administer drugs.
- **Miscommunication of Drug Orders:** Failed communication is at the heart of many errors. This includes poor handwriting, confusion of drugs with similar names, careless use of zeroes and decimal points, confusion of metric and apothecary systems, use of inappropriate abbreviations, ambiguous or incomplete orders, and, sometimes, conflicts between practitioners.
- **Problems with Labeling, Packaging and Drug**

Nomenclature: Most drugs are dispensed through unit dose systems that parse medications into smaller-sized doses. These systems, however, do not always provide for thorough preparation, packaging, and labeling of medications, with screening and checking by both nursing and pharmacy personnel, and they may not be available throughout every unit in the hospital (e.g., ERs and ICUs). Drug administration procedures often do not ensure that medications remain labeled until they reach the patient's bedside, a frequent source of error.

- **Drug Standardization, Storage, and Stocking errors:** Stocking multiple concentrations of the same drug, or storing drugs in look-alike containers or in ways that obscure drug labels, may contribute to error. Lack of Safety procedures for use of automated dispensing technology or inadequate check systems may also contribute to errors.
- **Drug Device Acquisition, Use and Monitoring:** Lack of standardization in drug delivery devices, improper default settings, unsafe equipment (e.g., free-flow infusion pumps), and the lack of independent check systems for verifying dose and rate settings can all contribute to device-related errors.
- **Environmental Stress:** Environmental factors like lighting, heat, noise, and excessive interruptions, can affect individual performance. The process of transcribing orders is particularly vulnerable to distractions in the environment, as staff are exposed to noise, interruptions, non-stop unit activity, and too-long or double shifts.
- **Limited Staff Education:** Many practitioners are not as aware as they should be of situations within their own organizations that have been reported as error-prone, or of similar information published in professional literature.

Quality Improvement Processes and Risk Management: Health facilities need systems for identifying, reporting, analyzing, and correcting errors and identifying trends, and measurement systems for tracking the effect of system changes. Also, organizations need to take into consideration information from outside sources about errors that have occurred elsewhere. But above all, health organizations need to cultivate a non-punitive approach to error that will encourage frank identification and analysis of errors when they occur.

Steps for Improving Medication Safety

These potential sources of error can be controlled if we design safer systems. With this in mind, the AHA has attached to this advisory a list of successful practices for improving medication safety and for improving overall patient safety within our hospitals and health systems. We encourage your team to review this list of recommendations, plan for implementation, and begin to track your progress.

Our Sources

The recommendations were culled from several reliable sources that are leaders in the effort to reduce and prevent medication errors, and we are grateful for their pioneering efforts. This list includes those organizations, as well as other resources for your organization's efforts.

- ✦ American Society of Health-System Pharmacists (www.ashp.org)
- ✦ American Society for Healthcare Risk Management (www.ashrm.org)
- ✦ Institute for Healthcare Improvement (www.ihl.org)
- ✦ Institute of Medicine (www.national-academies.org)
- ✦ Institute for Safe Medication Practices (www.ismp.org)
- ✦ Joint Commission on Accreditation of Healthcare Organizations (www.jcaho.org)
- ✦ Massachusetts Hospital Association (www.mhalink.org)
- ✦ Massachusetts Coalition for the Prevention of Medical Errors (www.mhalink.org/mcpme)
- ✦ National Coordinating Council on Medication Error Reporting and Prevention (www.nccmerp.org)
- ✦ National Patient Safety Foundation (www.npsf.org)
- ✦ U.S. Pharmacopeia (www.usp.org)

Books

- ✦ Cohen, Michael R., Ed. Medication Errors. Washington, D.C. American Pharmaceutical Association. 1999. (Contains a special chapter on high-alert medications and dangerous abbreviations; rich with insight and practical advice on reducing the risk of error.)
- ✦ Corrigan, Janet, et al. To Err is Human: Building a Safer Health System. Washington, D.C. National Academies Press. 1999. (Comprehensive overview of medical error, containing many practical suggestions and recommendations from several trusted sources.)
- ✦ Leape, Lucian, et al. Reducing Adverse Drug Events. Boston, MA: Institute for Healthcare Improvement. 1998 (Concepts to reduce adverse events and a model for improvement.)

Patient Information Brochures

- ✦ Your Role in Safe Medication Use: A Guide for Patients and Families is available from the Massachusetts Hospital Association at www.mhalink.org
- ✦ Partners in Quality: Taking an Active Role in Your Health Care is available from the Hospital & Health System Association of Pennsylvania at www.hap2000.org
- ✦ How to Take Your Medications Safely is available from the ISMP at www.ismp.org

- ✦ Just Ask! Is available from the U.S. Pharmacopeia at www.usp.org

Information on Safe Medication Practices From the Institute for Safe Me

Ensure the availability of up-to-date drug information

- Make updated information on new drugs, infrequently used drugs, and non-formulary drugs easily accessible to clinicians prior to ordering, dispensing, and administering medications (e.g., have pharmacists do rounds with doctors and nurses; distribute newsletters and drug summary sheets; use computer aids; and provide access to formulary systems and other internal resources).
- Review error potential for all new products, including a literature review, before any drug or procedure is approved for use; reassess six months to one year later

NC ASHRM BOARD 2001

Name/Mailing Address	NC ASHRM Title	E-mail	Work Phone	Work Fax	Home Phone
Thompson, Richard Dirctor, Risk Management Albemarle Hospital PO Box 1587 Elizabeth City, NC 27102	President NCASHRM	rthompson@albemarlehosp.org	252-384-4651	252-384-4381	
Borg, Rina NC ASHRM PO Box 72248 Durham, NC 27722-2248	Executive Assist.	Borg01@ACPUB.Duke.EDU	919-479-2098	919-471-9231	919-479-2098
Byrd, Lisa Risk Manager Southeastern Medical Ctr. P.O. Box 1408 Lumberton, NC 28359	Board Member Prof Development Committee Chair	byrd02@srmc.org	910-671-5586	910-671-519	
Elliott, Sheila Claim Analyst Caronia Corporation PO Box 147 Reidsville, NC 27328	Vice President Program Committee Chair	sheila.elliott@cna.com	336-634-0220	336-634-0215	336-342-5332
Eure, Thom Risk Manager Scotland Memorial Hospital P.O. Box 1408 500 Lauchwood Dr. Laurinburg, NC 28352	Board Member Legislative Committee Chair	Thom.Eure@scotlandhealth.org	910-291-7509	910-291-7419	
Hendrix, Bobbie Dir, DUHS Clin. Risk Mgmt Box 3811 DUMC Durham, NC 27705	Secretary	Hendr001@mc.duke.edu	919-684-3277	919-681-8618 cell: 919-218-5121	919-383-4911
Mantooth, Charles F. (Chuck) Account Executive McNeary Healthcare Services PO Box 220926 6525 Morrison Blvd Charlotte, NC 28222	Immediate Past President	mantoothc@mcneary.com	800-729-4149 cell: 704-460-4334	704-365-7114	704-782-1325
Musselman, Sharon Medical Protective 2000 Regency Pk, Ste 295 Cary, NC 27511	Treasurer	smusselman@medprotect.com	919-467-8370	919-380-1775	919-542-6251
Rhodes, Jean Coord, Quality Assurance Valdese General Hospital Valdese, NC 28690	Board Member Chapter Achievement Committee Chair	jmrhodes@vgh.org	828-879-7548	828-437-3959	
Temple, Michelle Risk Manager WakeMed 3000 New Bern Avenue Raleigh, NC 27610	Board Member PR/Marketing Committee Liason	mtemple@wakemed.org	919-350-8234	919-350-5892	919-783-5344

TIME

