

# Learning from Others

## Legal Aspects of Sharing Patient Safety Data Using Provider Consortia

Bryan A. Liang, MD, PhD, JD,\*†‡ Matthew B. Weinger, MD,\*† and Steven Suydam, MD, JD\*†

**Abstract:** The Institute of Medicine (IOM) report *To Err Is Human* indicated that provider collaborative approaches are important to prevent the repeat of avoidable errors. It also recognized their legal risks, but analysis has heretofore not been available to assist providers to pursue these approaches. Patient safety consortia are collaborative efforts that can promote safety. However, legal analysis indicates only federal research protection under Agency for Healthcare Research & Quality (AHRQ) appears sufficient to confine its use to intended safety efforts. Absent AHRQ protection, discovery rules and privilege laws could likely allow such information to be used in lawsuits. Health Insurance Portability and Accountability Act (HIPAA) privacy rules also create issues of liability. These results, and the need to allow members to join and leave consortia, indicate corporations may be the appropriate consortium structure. Federal legislation is needed to provide clear protection for provider sharing of safety information.

**Key Words:** medical errors, law, safety consortiums, sharing data, legal issues

(*J Patient Saf* 2005;1:83–89)

When an adverse event such as a patient's death due to an error or systems weakness occurs at one facility, it is in the public's interest for this information to be disseminated rapidly to all similarly situated providers. However, substantial underreporting and the near absence of data sharing among health care providers make it much more likely that there will be many additional unnecessary deaths before appropriate interventions occur. Recognizing this, the Institute of Medicine (IOM) report *To Err Is Human* recommended voluntary error reporting and safety efforts using collaborative approaches across providers to prevent the same errors from being repeated in different organizations.<sup>1</sup>

Provider safety consortia are one type of collaborative effort. Roughly half a dozen of these consortia in varying stages of development exist, including regional initiatives in

Pittsburgh, PA, Chicago, IL, Dayton, OH, Madison, WI,<sup>2</sup> and San Diego, CA. These consortia are formed by member health care institutions to exchange information, analyze data, and disseminate effective safety practices to reduce patient morbidity and mortality and improve quality. Typically, consortium members report medical errors and accidents to a central expert repository. There, the information is analyzed and lessons learned are disseminated back to provider members (and possibly others) for application in their own facilities. Such collaborations have great potential for learning from the experience of another's medical errors by pooling data to increase the power of any study and providing a wider range of cases from which to draw inferences regarding safety.

One significant obstacle to such consortium formation recognized in the IOM report is that institutional exchange of information may render it vulnerable to legal discovery for use in medicolegal proceedings. The report recommended that federal legislation was needed to address this concern. Such legislation should extend peer review protections to data and discussions related to safety and quality improvement collected and analyzed by health care organizations for internal use. The report also noted that, importantly, such protections should also include information shared with others solely to improve safety and quality.<sup>1</sup> While federal bills consistent with this recommendation have been proposed, none have become law. The report also suggested that state law, more specifically state peer review/quality assurance (PR/QA) privilege, could provide protection for exchanging safety data between institutions.<sup>1</sup>

Providers interested in forming consortia to study error and promote safety, however, have had little guidance regarding issues that must be considered when initiating such an effort. We, therefore, assessed some of the key legal concerns regarding the formation of patient safety consortia by first evaluating available federal statutory protections for research data, including Agency for Healthcare Research & Quality (AHRQ) confidentiality provisions (known as the "299c-3(c) provision")<sup>3</sup> and certificates of confidentiality under the Public Health Service Act (known as the "241(d) provision")<sup>4</sup>; legal discovery rules; and state privilege laws. HIPAA (Health Insurance Portability and Accountability Act) is also reviewed in relation to consortium activities, and possible legal structures that relate to individual member liability concerns using HIPAA as an example are assessed. We conclude with recommendations for forming these safety consortia and a brief discussion of some federal policy considerations to permit their broader use.

From the \*San Diego Center for Patient Safety, University of California, San Diego School of Medicine; †Institute of Health Law Studies, California Western School of Law; and ‡Department of Anesthesiology, University of California, San Diego School of Medicine, San Diego, California.

Correspondence: Professor Bryan A. Liang, MD, PhD, JD, Executive Director, Institute of Health Law Studies, 350 Cedar Street, San Diego, CA 92101 (e-mail: baliang@alum.mit.edu).

Copyright © 2005 by Lippincott Williams & Wilkins

## RISKS OF SHARING INFORMATION RELEVANT TO PATIENT SAFETY

Although there are substantial benefits to sharing patient safety data among health care entities, including description of systemic circumstances surrounding patient care accidents and safety improvement activity outcomes, the risks are considerable. The greatest perceived risk is likely medicolegal. This risk encompasses not only the revealing of a specific adverse patient event that then might be subject to legal action, but also the potential for unintended waiver of evidentiary privilege, that is, protection of materials from being subject to the discovery process. Other legal, reputational, and financial concerns may also attend. Hence, there is great concern to ensuring safety information be limited to its intended use.

## POTENTIAL FEDERAL PROTECTIONS

Generally, if a patient injury occurs, patients, through their attorneys, will seek any information that may be persuasive in establishing provider negligence. Thus, allowing safety effort information, including reporting and analyses of important data about medical accidents to improve system safety, to be discoverable to support lawsuits could chill all safety efforts. However, although originally intended for protection of clinical researchers against disclosure of patient data, premature disclosure of research results, and other non-academic uses, two federal research protections may promote safety activities by confining this information to its intended safety use.

### 299c-3(c) Provision

The AHRQ authorizing statute specifically provides limits on research information dissemination:

■ (c) *Limitation on use of certain information.*

*No information, if an establishment or person supplying the information or described in it is identifiable, obtained in the course of activities undertaken or supported under this subchapter may be used for any purpose other than the purpose for which it was supplied unless such establishment or person has consented (as determined under regulations of the Director) to its use for such other purpose. Such information may not be published or released in other form if the person who supplied the information or who is described in it is identifiable unless such person has consented (as determined under regulations of the Director) to its publication or release in other form.*<sup>5</sup>

Hence, disclosure or use of any information or information “in other form” apart from the specified purpose indicated by AHRQ grant/sponsorship is impermissible, provided the reporter, that is, the “establishment ... supplying the information,” or subject “described in it,” is identifiable.

This provision is highly applicable to safety reports and dissemination in safety consortia. Protected “information” would be error reports and data from members. Information “in other form” would be repository analyses and feedback to members of the safety consortium, and others, if they were within the intended scope of the AHRQ project.

Further, another provider concern is addressed by 299c-3(c)—the confidentiality of member reporter identities. For a specific health care facility, serious adverse events are rare. Thus, disclosure of its report and analysis would likely identify the “establishment ... supplying the information or described in it ...”<sup>6</sup> This is particularly true in rural and non-urban communities.<sup>7</sup> Hence, by the very nature of error and adverse event epidemiology, AHRQ protection could be available for all safety consortium information: member reports, repository feedback, and the identity of those who provided the reports.

AHRQ general guidance supports this conclusion. An AHRQ advisory memorandum indicates that information reported to an AHRQ researcher/organization would likely be protected from legal discovery, at least from the AHRQ researcher/organization.<sup>6</sup> This same memorandum warns that when reporters who simply provide non-identifiable patient information to AHRQ grantees and are not themselves identified by the report (such as hospitals who provide treatment results of their patients with HIV), reporters may lose any protections against legal discovery due to their disclosure of the information outside the facility. However, because safety consortium reports may either be “information” or information “in other form” within the statute, and disclosure would likely identify the reporter due to the rare nature of medical accidents per provider, safety reports, analysis, feedback, and reporter identities should also fall within the statutory protections.

Note that no court has yet ruled on the applicability of the 299c-3(c) protections to safety information or, specifically, consortium efforts. However, at a minimum, AHRQ-funded repositories for data collection could have protection from disclosure of data, member identities, and safety communications for non-AHRQ purposes. Attorneys seeking information on a specific patient injury would be limited to requesting standard malpractice information, such as patient charts, directly from the health care provider.<sup>8</sup>

### 241(d) Provision (Certificates of Confidentiality)

The Public Health Act under section 241(d) also contains a provision granting researcher protection:

■ (d) *Protection of privacy of individuals who are research subjects.*

*The Secretary may authorize persons engaged in biomedical, behavioral, clinical, or other research (including research on mental health, including research on the use and effect of alcohol and other psychoactive drugs) to protect the privacy of individuals who are the subject of such research by withholding from all persons not connected with the conduct of such research the names or other identifying characteristics of such individuals. Persons so authorized to protect the privacy of such individuals may not be compelled in any Federal, State, or local civil, criminal, administrative, legislative, or other proceedings to identify such individuals.*<sup>9</sup>

This provision was created in part to encourage patient participation in studies on sensitive topics such as alcohol abuse and AIDS-related research.

This statutory provision is significantly less applicable to safety research using consortia. First, although it expressly applies to legal proceedings, its primary focus is the protection of individual patient/subject identities, and by exclusion as compared with 299c-3(c), not an “establishment” reporter such as an institution. Further, it is highly likely that data is not protected by this statute. Federal courts have allowed for data discovery from research entities even in the presence of 241(d) protection when patient identities are redacted.<sup>10,11</sup> Since adverse events per facility are rare, even with patient identities redacted, reporter identities will be apparent. Hence, it is unlikely that either member-reported data and information or reporter identities would be protected from discovery under the 241(d) provision.

### LEGAL DISCOVERY RULES

Legal discovery is the method by which evidence is produced for lawsuit purposes from those who possess it.<sup>12</sup> For example, the Federal Rules of Civil Procedure, which govern federal civil lawsuit claims and have been adopted in most states for their own courts, indicate parties have the right to information regarding any matter relevant to the case not protected by a specific evidentiary privilege.<sup>13</sup> Indeed, information discoverable need not even be admissible at trial. Such information simply needs to be “reasonably calculated” to lead to the discovery of admissible information.<sup>14</sup> Further, the U.S. Supreme Court promulgated “automatic disclosure requirements” that require parties in a civil suit at the outset of the case, and without request by the other party, to produce “a copy of, or a description by category and location of, all documents, data compilations, and tangible things in the possession, custody, or control of the party that are relevant to [the case].”<sup>15</sup> For safety consortium members, absent 299c-3(c) privilege protection, reports and information communicated between consortium members and consortium repositories would be subject to legal discovery from both. Courts would likely deem such reports and information as directly relevant to a patient injury suit and subject to discovery, and, indeed, even within the automatic disclosure requirements. Here 241(d) protection is unhelpful; any privacy protected under this provision would be waived by the patient to allow for its use in the lawsuit.

This situation highlights the importance of the AHRQ 299c-3(c) provision. It would likely act as an evidentiary privilege precluding discovery of safety data and information, reporter identities, the member reports, and consortium member feedback. Note, however, that discovery can still reach traditional patient injury suit materials, for example, patient charts, when requested from individual providers.

### STATE PRIVILEGE LAWS

#### Peer Review/Quality Assurance Privilege

The IOM report indicated that PR/QA privilege is a source of protection for sharing patient safety information. All states have adopted some form of PR/QA privilege.<sup>16</sup> It generally encompasses provider assessment of care delivery and internal quality reviews. However, it is doubtful that PR/QA

privilege will protect consortium information, reporter identities, or member reports from legal discovery.

First, state PR/QA laws focus upon traditional QA and PR activities. However, patient safety research projects would likely not fall within the standard definition of PR/QA on the basis of analysis of PR/QA laws and court holdings.<sup>17</sup> In addition, safety work is usually deemed “research” rather than quality improvement, which also places it into a different legal domain.<sup>18</sup>

Second, state PR/QA statutes vary significantly. Some only apply to specific entities (eg, hospitals), some do not include for-profit entities, some only apply to non-managed care organizations, and importantly, some do not cover third party entities contracting with a provider to assist in performing QA.<sup>19</sup> This latter situation appears to directly apply to safety consortium members and repositories engaged in safety research.

Third, courts have been narrowing the scope of PR protections,<sup>20</sup> consistent with U.S. Supreme Court jurisprudence expressly disfavoring PR-based discovery limitations<sup>21</sup> and other Supreme Court decisions limiting evidentiary privilege.<sup>22,23</sup> PR/QA privilege is also not considered absolute: “[i]f a trial court determines that the success or failure of a litigant’s cause of action or defense would likely turn on the evidence adjudged to fall within the scope of [PR/QA privilege], then the trial court shall compel production of such evidence.”<sup>24</sup>

To afford itself of the PR/QA privilege, the relevant body must perform traditional PR and QA activities,<sup>25</sup> and that must be its “primary function.”<sup>26</sup> An entity cannot simply deem any member of its staff as part of a “PR/QA Committee” in an effort to extend the privilege.<sup>27</sup> Further, disclosure of information gleaned in PR/QA deliberations to third parties may vitiate the privilege<sup>28,29</sup>; courts have held that PR/QA privilege of one entity does not apply to other institutions, and disclosure to third parties has been expressly found to waive the privilege.<sup>30</sup> Indeed, even partial PR information disclosure can waive any previously existing privilege.<sup>31,32</sup>

Finally, PR/QA privilege is state-based. Hence, under jurisdictional rules, any cause of action involving federal law will generally not be subject to state law privileges, including PR/QA. If a malpractice claim, which is generally a state law claim, is pled with a federal cause of action, such as EMTALA violation, federal antitrust, consumer protection, or discrimination law, or other federal claim, then the federal court may take jurisdiction over the state malpractice claim. In this circumstance, federal evidentiary and privilege rules would apply, thus eliminating any protections of state PR/QA privilege.<sup>18</sup> This is consistent with the federal Healthcare Quality Improvement Act, which provides qualified immunity to PR/QA participants, but not to any PR/QA materials.<sup>33</sup>

#### Attorney-Client Privilege and Work-Product Doctrine

Attorney-client privilege protects communications between attorneys and clients to allow full candor so the attorney may best advise his/her client. Providers and risk managers may sometimes believe that the attorney-client privilege may protect safety information from discoverability because safety

information is related to patient injury. However, two major weaknesses of this privilege make it inapplicable to safety information and reporting.

First, as in PR/QA, any disclosure of the information to third parties waives the privilege.<sup>34,35</sup> Hence, error and data reports by a consortium member will likely waive any possible privilege the member might have had if dissemination were limited to its attorney. Second, and critical for safety consortia, if information to be protected is discussed for any reason *other than* in preparation for litigation—such as for safety purposes—the information is discoverable because dissemination has gone beyond the traditional rationale of the privilege.<sup>36</sup>

Similarly, work product protection does not provide safety consortium information safeguards for unintended use. Work product represents an attorney's preparation for a client's case,<sup>37</sup> that is, an attorney's litigation strategy, and is generally not discoverable. Again, some facilities and individuals may believe that since safety information is related to patient injury, it can be protected from discovery through having an attorney present at safety consortium meetings or through providing safety consortium communications to him/her and having the information be considered work product. However, it is unlikely that consortium member reports and repository analysis and feedback would be considered an attorney's preparation for litigation. Further, note that the mere presence of an attorney during data and information discussion, reporting, and assessment is insufficient to invoke work product protections,<sup>38</sup> and if documents to be protected are created in the normal course of business, they are not considered work product.<sup>39</sup>

Importantly, an assessment of discovery issues also implicates the use and disclosure of specific patient information, which raises the issue of patient information privacy. Because of the epidemiology of error, and the potential for identifiability of a particular patient when analyzing system weaknesses, HIPAA medical privacy provisions apply. These privacy provisions are assessed in relation to patient safety consortium efforts.

### HIPAA MEDICAL PRIVACY PROVISIONS

Error reports and data analysis in a safety consortium disclose and use patient information; hence, HIPAA medical privacy provisions apply.<sup>40</sup> HIPAA covers all patient-identifiable health care information/"protected healthcare information" (PHI), in any form maintained or transmitted by "covered entities," including providers, contractors, subcontractors, and health plans. In addition, these entities' business associates are subject to the privacy rules, including those who provide consulting, management, data aggregation, and other services to covered entities. Contracts between these parties must limit business associate use/disclosure of patient information to parties specified and must require specific security, inspection, and reporting mechanisms by business associates and by business associate subcontractors. Internal records must be made available to the Secretary of the Department of Health and Human Services (DHHS) if requested, and all protected information must be returned or destroyed at the end of the contract period if practicable. The covered entity may be held

responsible for rule violations of its business associates if it has knowledge of these violations.

Penalties for HIPAA violations are severe. Both civil monetary penalties of up to \$25,000 and criminal penalties of up to 10 years' imprisonment and fines of up to \$250,000 may be imposed for each standard violation. HIPAA represents a floor of medical privacy protection; stricter state laws and sanctions are not preempted.

For non-treatment, payment, or health care operations, covered entities that wish to use/disclose PHI for safety efforts must generally obtain HIPAA patient authorization, a quite involved process. Notably, providers cannot perform safety research under the "healthcare operation" provision. Although regulations indicate health care operations expressly include "quality assessment and improvement," they expressly note that health care operations *do not* encompass studies that result in "generalizable knowledge."<sup>7</sup>

There are three exceptions to patient authorization requirements: health oversight activities, public health activities, and research. Health oversight and public health exceptions only encompass public or governmental agencies, leaving only research for most entities interested in safety work.

Yet the research exception appears to apply most readily to traditional clinical research, since the rule consistently provides only clinical trials as examples and does not mention patient safety or systems performance research. The rule does, however, outline two mechanisms by which a covered entity can demonstrate meeting the research exception: having someone with "appropriate knowledge and experience" in statistics indicate that "the risk is very small that the information could be used ... to identify the subject"; or deidentification, that is, removing 19 specific patient identifiers from the patient's records. This latter provision may be most applicable to patient safety consortia, particularly since the procedure for demonstrating the former is not defined and previous analysis points to some risks associated with the knowledge/experience documentation approach.<sup>7</sup> However, it should be emphasized that the lack of case law and legal guidance may make either approach acceptable. In any event, materials should be deidentified using either approach so that materials used for safety analysis cannot identify the individual patient.

Hence, to avoid the need to obtain authorization from all patients whose information is used/disclosed in safety consortium and potential HIPAA liability, both members and the repository must ensure that records are appropriately deidentified, with close attention to HIPAA's requirements. Further, since it is likely that a consortium member acting as a repository for member reports will be considered a business associate, contractual arrangements between the two must memorialize HIPAA compliance.

### THE LEGAL STRUCTURE OF PATIENT SAFETY CONSORTIA

A patient safety consortium may be an independent legal entity, or simply an association of providers who agree to share information to promote safety. However, an individual provider concern that arises is the potential for liability associated with consortium actions. For example, inappropriate use of PHI

may invoke severe penalties under HIPAA. Hence, attention to legal structures is important to limit this risk, particularly for consortium repositories.

There are a number of legal structures through which a consortium may choose to organize and act: for example, an informal nonincorporated entity, a formal corporation structure, and a partnership model.

In general, partnerships are legal entities with joint ownership and individual partner authority to act in the name of and bind the partnership. As well, partnership liability reaches all members of the partnership for actions of a single partner.<sup>41</sup> Further, if any individual partner leaves or any new partner enters, the original partnership is dissolved and a new partnership must be formed.<sup>42</sup>

As applied to patient safety consortia, partnerships are of limited value. It is unlikely that any member would wish to be bound by action of another consortium partnership member. Further, the high transaction costs associated with re-creating a partnership any time a member is to be added or one leaves would not be cost-effective. Third, since all partners share in liability personally, any action of, say, the repository or reporter member that violates HIPAA would reflect onto all partnership members.

The unincorporated nonprofit association may be a viable alternative. In general, these associations base member relationships on contract, whether by individual written contracts with specified terms, or by implied contract through their actions that may not be formally written. Each party to the contract is an independent entity, and there are no legal entities other than the contracting parties. Adding members to the consortium would be a matter of agreeing to specified terms in oral or written form; members who wish to withdraw simply invoke termination procedures specified by their agreement.

Any liability concerns will generally be focused upon the discrete individual entities,<sup>43</sup> unless the association is for-profit, in which case it would likely be considered a partnership.<sup>44</sup> Once again, using HIPAA, any liability associated with inappropriate PHI use/disclosure would be limited to the offending party(ies). Any other member of the association would generally not be implicated in HIPAA liability for the actions of the offending reporter and repository. But, under this structure, liability is not limited; any and all assets of the offending party may be reached to satisfy legal penalties.

The most protective legal structure for a safety consortium may be the corporation. Consortium members may form a corporation to collect and analyze safety information submitted by members. Alternatively, a single member, perhaps most appropriately the member acting as the repository, may create the corporation and allow other members to affiliate with it, either through purchase of corporate shares or by contract. Either approach allows for simple addition of new members. Assuming that corporate formalities are fulfilled (ie, corporate accounting, judgment, and decision-making rules are adhered to; no insider trading, etc.—issues unlikely to be of great risk to a safety consortium), the corporation (rather than any individual consortium member) may formally collect safety information, act as a repository, analyze data, and communicate lessons back to members. An entity may act as both a member representative (eg, reporter) and as a corpo-

ration representative (eg, repository), again as long as corporate formalities are followed.

Importantly, with regard to liability, if the corporate repository member is sued, for example under HIPAA, only the corporation's assets can be reached for liability; assets of the individual member acting as the repository cannot generally be reached.<sup>45</sup> And only if a member reporter has actual knowledge of repository violation and does not act to remedy the circumstances would the individual reporter be subject to HIPAA liability for repository actions. Of course, if an individual reporter consortium member violates HIPAA, it can always be reached. However, no other member will share liability in this circumstance, whether the corporation is implicated or not.

## RECOMMENDATIONS FOR CREATING PATIENT SAFETY CONSORTIA

### Obtain 299c-3(c) Protection

AHRQ statutory protection likely represents the greatest source of protection of safety data, reporter identities, and information reported to consortium repositories and fed back to members. Further, the AHRQ provision also addresses the fact that even if patient PHI is appropriately deidentified under HIPAA, the consortium member reporter may still be identifiable. Because 299c-3(c) expressly notes that if the "establishment" supplying the information, not only the patient, is identifiable, the information cannot be released for non-AHRQ purposes. Hence, deidentification that fulfills the HIPAA privacy rule will likely not vitiate AHRQ protections. Further, 299c-3(c) protection would likely be considered a privilege against discovery under civil procedure rules, which may also preclude attorney efforts to obtain data or the results of analyses to support lawsuits, as has been attempted in the past.<sup>46</sup> However, 299c-3(c) protection will not preclude discovery of traditionally discoverable materials, such as the patient's chart.

### Seek Out State-Specific Privilege Information

Although unlikely to provide broad protections for safety consortium members exchanging information generally, state-specific PR/QA and other privileges may offer some protections as defined by that particular state's law and the consortium's specific circumstance. For example, a "carve out" within existing state PR/QA laws to specifically protect sharing of patient safety data among regional or statewide institutions may exist. In California, trauma care under Evidence Code §1157.7 has been carved out in this manner, facilitating the creation of regional trauma networks and substantial improvements in trauma care through sharing of patient outcomes and quality improvement strategies.<sup>47</sup> In other states, there are specific discovery protections for patient safety data.<sup>48,49</sup>

### Fulfill the Research Deidentification Safe Harbor of HIPAA

To avoid the severe penalties of HIPAA, as well as the high costs of individual authorization for PHI use/disclosure, HIPAA deidentification should be complied with in all consortium information transfer and sharing. Such deidentification

under the privacy rule will likely not eliminate 299c-3(c) protections. It is equally important to deidentify providers and institutions in data submitted to the data repository or shared among consortium members; such deidentification may provide an additional barrier to preclude safety information unintended use.

### The Consortium Should Create a Legal Structure

Consortium members and, in particular, members acting as the repository, should carefully consider under what specific legal structure they wish to operate. The corporation is likely to be most effective to limit the liability and protect the assets of any member acting as the repository of safety information. Unincorporated associations using member contracts may be an acceptable alternative, but liability is not limited and all assets of the repository member may be reached to satisfy any legal judgment/penalty. No legal structure will prevent a plaintiff from suing an individual provider and obtaining standard discoverable information.

### FEDERAL POLICY IMPLICATIONS

The above analysis has several policy implications. First, although there may be avenues through which safety consortium activities can be performed, at present, AHRQ statutory protection appears to be critical for broad promotion of collaborative approaches. AHRQ initial funding of a number of developing centers of patient safety was an appropriate strategy to provide the necessary protections to allow safety work to be performed. However, recent AHRQ funding limitations and an almost exclusive focus upon information technology create difficult issues for safety consortia that require AHRQ sponsorship and funding to avail themselves and their members of the needed protections to substantively encourage and engage in these cross-institutional safety efforts. AHRQ recently announced an RFA for a contract to identify and support statewide data sharing and interoperability activities aimed at improving the quality, safety, efficiency, and effectiveness of health care for patients and populations on a discrete state or regional level.<sup>50</sup> It would be greatly helpful if such funding, even in smaller amounts, were allocated to safety consortia to allow for AHRQ protections to be widely available to accelerate the dissemination of safety research and lessons learned across health care institutions.

Even with AHRQ sponsorship, however, the legal protections discussed here have not been tested nor applied to safety consortia. As noted in the IOM report, the most effective solution would be passage of federal legislation protecting safety research reports, results, and lesson feedback to providers. Federal legislation, such as the Patient Safety Quality Improvement Act of 2003, Senate Bill 720, would be a highly effective statute to fulfill this need and provide the impetus and infrastructure for safety consortia.

Finally, of course, increased funding for safety research and consortium efforts, including best practices regarding the structure of safety consortia, would facilitate rapid advancements in safety that may be confidently shared across providers, increasing participation and learning. By understand-

ing the best means through which consortia can collect, analyze, and disseminate patient safety information across institutional boundaries, the most effective and efficient use of the research dollar and patient safety can be advanced.

### ACKNOWLEDGMENTS

Bryan A. Liang, MD, PhD, JD, was supported in part by the Agency for Healthcare Research & Quality (U18HS11905-01); and Matthew B. Weinger, MD, was supported in part by the Agency for Healthcare Research & Quality (P20 HS11521-03).

### REFERENCES

1. Institute of Medicine. *To Err Is Human: Building a Safer Health System*. Washington, DC: Institute of Medicine; 2000.
2. Agency for Health Care Research & Quality. *AHRQ's Patient Safety Initiative: Building Foundations, Reducing Risk: Interim Report to the Senate Committee on Appropriations*. AHRQ Publication No. 04-RG005, December 2003. Available at: <http://www.ahrq.gov/qual/pscongrpt/index.html#Contents> (last visited January 25, 2005).
3. 42 U.S.C. § 299c-3(c).
4. 42 U.S.C. § 241(d).
5. 42 U.S.C. § 299c-3(c).
6. Center for Quality Improvement and Patient Safety, Agency for Healthcare Research and Quality. *Statutory Confidentiality Protection of Research Data: Memorandum from Susan Greene Merewitz*, Apr. 16, 2001. Available at: <http://www.ahrq.gov/fund/datamemo.htm> (last visited June 15, 2004).
7. Liang BA. The adverse event of unaddressed medical error: identifying and filling the holes in the health-care and legal systems. *J Law Med Ethics*. 2001;29:346-368.
8. Liang BA. Risks of reporting sentinel events. *Health Aff (Millwood)*. 2000;19:112-120.
9. 42 U.S.C. § 241(d).
10. *Murphy v. Philip Morris Inc.*, 1999 WL 3521196 (C.D. Cal. Dec. 28, 1999).
11. *Wolpin v. Philip Morris, Inc.*, 189 F.R.D. 418 (C.D. Cal. 1999).
12. Glannon J. *Civil Procedure, Examples and Explanations*. 3d ed. New York: Aspen; 1997.
13. Rule 26(b). *Federal Rules of Civil Procedure*. St. Paul: West Publishing; 2002.
14. Rule 26(a). *Federal Rules of Civil Procedure*. St. Paul: West Publishing; 2002.
15. Rule 26(a)(1)(B). *Federal Rules of Civil Procedure*. St. Paul: West Publishing; 2002.
16. Scheutzw S. State medical peer review: high cost but no benefit—is it time for a change? *Am J Law Med*. 1999;25:7-60.
17. Liang BA. Error in medicine: legal impediments to U.S. reform. *J Health Polit Policy Law*. 1999;24:27-58.
18. Lynn J. When does quality improvement count as research? Human subject protection and theories of knowledge. *Qual Saf Health Care*. 2004;13:67-70.
19. Liang BA, Storti K. Creating problems as part of the "solution": the JCAHO sentinel event policy, legal issues, and patient safety. *J Health Law*. 2000;33:263-285.
20. Cepelewicz B, Dunn L, Felch D, et al. Recent developments in medicine and law. *Tort Insur Law J*. 1998;33:583-603.
21. *Univ. of Pennsylvania v. EEOC*, 493 U.S. 182 (1990).
22. *Trammel v. U.S.*, 445 U.S. 40 (1980).
23. *42 U.S. v. Nixon*, 418 U.S. 683 (1974).
24. *Southwest Comm. Health Services v. Smith*, 755 P.2d 40 (N.M. 1988).
25. *Freeman v. Piedmont Hosp.*, 444 S.E.2d 796 (Ga. 1994).
26. *Claypool v. Mladineo*, 724 So.2d 373 (Miss. 1998).
27. *Franzen v. Children's Hosp. of Wisconsin*, 485 N.W.2d 603 (Wis. App. 1992).
28. Scheutzw S, Gillis S. Confidentiality and privilege of peer review information: more imagined than real. *J Law Health*. 1992/1993;7:169-197.

29. Bremer W. Scope and extent of protection from disclosure of medical peer review proceedings relating to claim in medical malpractice action. In *American Law Reports*. 5th ed. St. Paul: West Publishing; 2004.
30. Terrell v. Ashcroft, 794 S.W.2d 937 (Tex. App. 1990).
31. Whitman by Whitman v. U.S., 108 F.R.D. 5 (D.N.H. 1985).
32. Riney T, Wolek C. Hippocrates enters the new millennium—Texas medical privileges in the year 2000. *S Texas Law Rev*. 2000;41:315–369.
33. 42 U.S.C. § 11101 *et seq*.
34. Chicago Trust Co. v. Cook Cty. Hosp., 698 N.E.2d 641 (Ill. App. 1998).
35. State of West Virginia *ex rel* United Hosp. Ctr., Inc. v. Bedell, 484 S.E.2d 199 (W.Va. App. 1997).
36. State of W.Va. *ex rel* United Hosp. Ctr., Inc. v. Bedell, 484 S.E.2d 199 (W.Va. App. 1997).
37. Hickman v. Taylor, 329 U.S. 495, 510-11 (1947).
38. Warleigh v. Second Judicial Dist. Ct., 891 P.2d 1180 (Nev. 1995).
39. Stout v. Illinois Farmers Ins. Co., 150 F.R.D. 594 (S.D. Ind. 1993), *aff'd*, 852 F. Supp. 704 (S.D. Ind. 1994).
40. 45 C.F.R. Parts 160, 164 (2003).
41. Kansallis Finance Ltd. v. Fern, 659 N.E.2d 731 (Mass. 1996).
42. Browne v. Ritchey, 559 N.E.2d 808 (Ill. App. 1990).
43. Heleniak v. Blue Ridge Ins. Co., 162 A.D.2d 1041, 557 N.Y.S.2d 229 (4th Dep't 1990).
44. Shortlidge v. Gutoski, 484 A.2d 1083 (N.H. 1984).
45. Haberle A, Jones J, Levin J, et al. Powers, functions, and liabilities of corporations. In *American Jurisprudence Corporations*. 2nd ed. St. Paul: West Publishers; 2003:vol. 18B, ch. XVII.
46. Black B. Subpoenas and science—when lawyers force their way into the laboratory. *N Engl J Med*. 1997;336:725–727.
47. Cal. Evid. Code §1157.7 (2004).
48. Va. Code Ann. §8.01-581.7 (2002).
49. Fla. Stat. §766.101 (2003).
50. Agency for Healthcare Research and Quality. *State and Regional Demonstrations in Health Information Technology. Request for Proposals*. Rockville, MD: Agency for Healthcare Research and Quality; May 2004. Available at: <http://www.ahrq.gov/fund/rfp040015.htm> (last visited June 15, 2004).