# COLLABORATING ON PATIENT SAFETY: LEGAL CONCERNS AND POLICY REQUIREMENTS

BRYAN A. LIANG, M.D., PH.D., J.D.*

## I. INTRODUCTION

If an adverse event occurs due to an error or systems weakness, or a systems issue is identified and/or the best practices that address it are determined, then patients and providers benefit most if this information is disseminated broadly. This ensures the maximum possible learning across health delivery systems so that proactive systems improvements can make health care delivery safer and lessons need not be learned separately by each provider.

Yet under-reporting and the near absence of data sharing between healthcare providers is the rule rather than the exception. Regardless of whether the information is extant, if it is held in the hands of one provider on the basis of its own experience, it is likely to stay there. Recognizing this, the Institute of Medicine ("IOM") Report, *To Err is Human*, recommended voluntary error reporting and safety efforts using collaborative approaches between providers to prevent the same errors from being repeated by different organizations.[1] In other words, an emphasis upon collective learning would best promote patient safety across delivery systems in the United States.

Provider safety consortiums are one method of collaboration. Member healthcare entities formed these consortiums to exchange information, analyze data, share lessons learned, and disseminate effective safety practices and principles that reduce patient morbidity and mortality and improve quality of care.

In one model of consortium activity, consortium members report medical errors and/or accidents to a central expert repository, where the information is analyzed, and lessons learned are disseminated back to provider members (and possibly others) for application in their own facilities. Another model is to have collaborations where a specific department or other focused unit's errors and/or system weaknesses have been addressed. The lessons learned through analysis

---

* Executive Director and Professor of Law, Institute of Health Law Studies, California Western School of Law, San Diego, CA; Co-Director and Adjunct Associate Professor of Anesthesiology, San Diego Center for Patient Safety, University of California, San Diego School of Medicine, San Diego, CA; Adjunct Associate Professor of Public Health, College of Health & Human Services, San Diego State University, San Diego, CA.; B.S. MIT; Ph.D. University of Chicago; M.D. Columbia University College of Physicians & Surgeons; J.D. Harvard Law School. This work was presented at Regulating Medical Errors, Widener University School of Law, Wilmington, DE, October 15, 2004. I thank the members of that forum for helpful suggestions and communications. Dr. Liang was supported in part by the Agency for Health Care Research & Quality (grant U18 HS11905-01). Dr. Liang assisted in crafting and supporting the Patient Safety and Quality Improvement Act and testified at a closed Senate Health Education Labor and Pensions committee briefing on this topic.

1. *See* IOM, TO ERR IS HUMAN: BUILDING A SAFER HEALTH SYSTEM 86-108 (Linda T. Kohn et al. eds., 2000).

of those errors and/or system weaknesses are then shared amongst members, facilitated by a central expert member. Such collaboration models have great learning potential gained through the experience of another's medical errors and approaches used to address them.[2] They also provide a wider range of cases and experiences from which to draw inferences regarding safety.

Both of these approaches provide consortiums with great potential to improve safety through group learning. In this manner, both system weaknesses and system improvements are utilized to enhance and promote continuous safety and quality improvement in and across health care delivery systems.

However, one significant obstacle to consortium activities recognized in the IOM Report is that institutional exchange of information may render it highly vulnerable to legal discovery for use in medical-legal proceedings.[3] Indeed, this potential risk of safety information used for non-safety purposes is a critical concern of providers in performing patient safety activities.[4]

To address this concern, the IOM Report recommended that federal legislation be enacted to extend peer review protections to data and discussions related to safety and quality improvement, collected and analyzed by healthcare organizations for internal use, or shared with others solely to improve safety and quality.[5] The Report also suggested that a state peer review/quality assurance ("PR/QA") privilege could provide protection for the exchange of safety data between institutions.[6]

Although the IOM Report made these recommendations, it provided few useful details on how to structure data sharing efforts between health care entities. Specifically, providers interested in forming consortiums to study error and promote safety had little, if any, guidance regarding issues that should be considered when initiating data sharing efforts. This article, therefore, assesses some of the key legal concerns regarding the formation of patient safety consortiums.[7]

In Part II, the article first indicates the risks associated with sharing patient safety data from a legal point of view and then evaluates available federal statutory protections for research data, including the Agency for Healthcare Research & Quality ("AHRQ") confidentiality provisions (known as the "299c-3(c)" provision),[8] and Certificates of Confidentiality under the Public Health

---

2. These models are broad approaches informally discussed by patient safety personnel.

3. IOM, *supra* note 1, at 109-10.

4. Bryan A. Liang, *The Adverse Event of Unaddressed Medical Error: Identifying and Filling the Holes in the Health-Care and Legal Systems*, 29 J.L. MED. & ETHICS 346 (2001).

5. IOM, *supra* note 1, at 109-31.

6. *See id.*

7. This analysis resulted from the San Diego Center for Patient Safety, University of California, San Diego School of Medicine's initiative to form a safety consortium among local hospital providers.

8. 42 U.S.C. § 299c-3(c) (2000).

Service Act (known as the "241(d)" provision).[9] In Part III, the article reviews the general legal discovery rules and state privilege laws, including PR/QA privilege, attorney-client privilege and work product doctrine and discusses how they might apply to patient safety activities. In Part IV, critical Health Insurance Portability and Accountability Act ("HIPAA") issues and their relation to consortium activities are assessed. On the basis of this analysis, in Part V, possible legal structures that relate to individual member liability concerns using HIPAA as an example are suggested. Part VI of the article reviews the newly enacted Patient Safety and Quality Improvement Act. Part VII provides a review of recommendations for forming patient safety consortiums. Finally, Part VIII gives a brief discussion of some policy issues implicated by safety consortiums.

## II. RISKS OF SHARING PATIENT SAFETY INFORMATION

Significant patient care and operational delivery benefits arise from sharing patient safety data between healthcare entities. These include descriptions of systemic circumstances surrounding patient care accidents and safety improvement activity outcomes. But the concurrent risks are considerable. The greatest perceived risk to providers is legal. This risk encompasses not only revealing a specific adverse event that might be subject to legal action but also the potential for unintended waiver of evidentiary privilege against discovery of this information that otherwise would apply. Further, sharing success stories regarding a particular delivery system improvement that resulted from error reporting and its analysis also may lead to identification of a particular organization's weaknesses, and events that also could lead to or be used in lawsuits against that provider. Accordingly, both substantive information disclosure and potential provider identification are the focus of concern in engaging in safety activities. Other legal, reputational and financial concerns may attend also; hence, ensuring that safety information is limited to its intended safety use is paramount to providers before any kind of data sharing is considered.

### *A. Potential Federal Protections*

If a patient injury occurs, attorneys will seek any information that may be persuasive in establishing provider negligence to support their claim. Beyond traditionally available information, such as patient charts and operating room reports,[10] safety information that describes errors and care delivery analyses

9. 42 U.S.C. § 241(d) (2000).

10. Note that safety consortiums do not attempt to preclude disclosure of standard medical charts and other materials currently available. Instead, the focus is upon safety materials that attempt to improve delivery system function. It should be noted that the airline industry has some

would be highly sought after materials to support patient injury lawsuits. But allowing safety effort information, such as reports and root cause system analyses of critical data surrounding medical accidents that improve delivery system safety, to be discoverable for lawsuit purposes could result in significant disincentives to engage in this assessment and chill all safety efforts.

However, two well known available federal research protections, although originally intended for protection of dinical researchers against disclosure of patient data, premature disclosure of research results and other non-academic uses, may promote safety activities by confining this information to its intended safety use. These are the Agency for Healthcare Research & Quality ("AHRQ") protection,[11] and the United States Department of Health and Human Services ("DHHS") Certificate of Confidentiality.[12] Their potential for protecting consortium safety information is assessed below.

1. 299c-3(c) Provision

AHRQ is a granting agency of DHHS and provides research funds for a broad array of health care activities.[13] Some of these activities may involve important public health areas, including sensitive subjects from the perspective of the patient. As such, there is a need to ensure confidentiality of some information and its source to ensure participation in data collection in the Agency's funded research.

The AHRQ authorizing statute specifically provides limits on research information and source 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

---

protections for safety information, including Aviation Safety Reporting System reports and commercial data collection information for safety purposes. *See e.g.*, In re Air Crash Near Cali, Colombia on Dec. 20, 1995, 959 F. Supp. 1529, 1530 (S.D. Fla. 1,997).

11. AHRQ, http://www.ahrq.gov (last visited Dec. 22, 2005).

12. DHHS, http://www.dhhs.gov (last visited Dec. 22, 2005).

13. Background on AHRQ, http://www.ahrq.gov/about/budgtix.htm#background (last visited Oct. 28, 2005). Nearly eighty percent of AHRQ's 269.9 million dollar budget is awarded as grants and contracts to researchers at universities and other research institutions across the country. AHRQ Profile, http://www.ahrq.gov/about/profile.htm (last visited Jan. 28, 2006).

> identifiable unless such person has consented (as determined under regulations of the Director) to its publication or release in other form.[14]

Hence, disclosure or use of any information or information "in other form" beyond the specified purpose indicated by AHRQ grant or sponsorship is impermissible if the reporter, i.e., the "establishment . . . supplying the information," or subject "described in it," is identifiable.[15]

The 299c-3(c) provision is highly applicable to safety communications and dissemination in patient safety consortiums that are AHRQ sponsored or funded. Protected information could include error reports and data from members. Information "in other form" could include repository analyses and feedback to members of the safety consortium and others if they are within the intended scope of the AHRQ project.

Indeed, the 299c-3(c) provision also may address the confidentiality of member reporter identities. For any single healthcare entity, serious adverse events are rare; thus, disclosure of its report and analysis regarding a specific event likely would identify the "establishment . . . supplying the information or described in it. . . ."[16] This is particularly true in rural and non-urban communities where patient populations are smaller and communities are more intimate.[17] Hence, due to the epidemiology of error and adverse events, AHRQ protections likely would be available for a broad array of safety consortium materials including member reports, repository feedback and the identity of those who provided the reports.

AHRQ general counsel guidance supports this interpretation and conclusion. An AHRQ advisory memorandum indicates that information reported to an AHRQ researcher or organization likely would be protected from legal discovery from the AHRQ researcher or organization, assuming the requirements of identifiability of the subject or reporter are fulfilled.[18] In addition, the memorandum warns that when non-AHRQ research project reporters provide non-identifiable patient or provider information to AHRQ, grantees may lose any legal discovery protections due to disclosure of this information outside of the walls of the entity.[19] However, in the patient safety context, provider safety consortium reports may either be "information" or information "in other form," as indicated within the statute, *and* disclosure likely would identify the reporter

---

14. 42 U.S.C. § 299c-3(c) (2000).

15. *Id.*

16. Susan Greene Merewitz, *Statutory Confidentiality Protection of Identifiable Research Data, Collected With AHRQ Support* (2001), http://www.ahrq.gov/fund/datamemo.htm (last visited Nov. 19, 2005).

17. *See* Liang, *supra* note 4, at 356. *See also* Bryan A. Liang, *Patient Information Privacy: HIPAA Provisions and Patient Safety Issues*, HOSP. PHYSICIAN, July 2002, at 43.

18. Greene Merewitz, *supra* note 16.

19. *Id.*

due to the rare nature of medical accidents associated with individual providers.[20] As such, safety reports, analysis, feedback and reporter identities should fall within the AHRQ statutory protections.

Although this analysis appears robust, no court has ruled on the applicability of the 299c-3(c) protections to safety information or specifically to provider safety consortium efforts yet. Even under these constraints, at a minimum, AHRQ-funded repositories for safety data collection and analysis should not be compelled to disclose information, member identities or safety communications for non-AHRQ purposes. Attorneys seeking information on a specific patient injury would be limited to requesting standard discoverable information such as patient charts directly from the healthcare provider,[21] and they should not be able to reach safety analysis and information.

2. 241(d) Provision (Certificates of Confidentiality)

DHHS, through its various agencies and subsections, including the National Institutes of Health ("NIH"), also provides grant monies for research.[22] These research areas may involve significant areas of public health with topics that are individually sensitive and that may require confidentiality to promote participation such as AIDS and alcohol abuse related research.

In response to these concerns, the Public Health Act under section 241(d) contains a provision granting researcher and individual subject protection, known as the Certificate of Confidentiality provision:

> (d) Protection of privacy of individuals who are research subjects
>
> The Secretary [of the Department of Health and Human Services] 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.[23]

---

20. 42 U.S.C. § 299c-3(c) (2000).

21. Bryan A. Liang, *Risks of Reporting Sentinel Events*, HEALTH AFF., Sept./Oct. 2000, at 114-118.

22. *See* NIH Grants & Funding Opportunities, http://grants2.hih.gov/grants/index.cfm (last visited Oct. 28, 2005).

23. 42 U.S.C. § 241(d) (2000).

The Certificate of Confidentiality statutory provision is unlikely to be applicable to safety research using provider consortiums. Although it expressly applies to legal proceedings,[24] its primary focus is the protection of individual patient or subject identities, and by exclusion as compared to 299c-3(c), does not address an "establishment" reporter such as an institution or provider entity. Consequently, reporter identities will likely be unprotected and readily determinable.

Further, it is probable that data will not be protected by this statute. Federal courts, in fact, allowed data discovery from research entities,[25] even in the presence of 241(d) protection, when patient identities were redacted.[26]

These results are highly problematic for provider consortium safety research. As noted above, since the incidence of medical accidents per facility is low, if reports are discoverable even when patient identities are redacted, then reporter identities will be apparent. And since the protection extends expressly only to patient identities, identifiable providers will be reluctant to report. Because it is unlikely that either member-reported data and information or their identities would be protected from discovery under the 241(d) provision, this provision would be unhelpful to patient safety consortium efforts and would not encourage data sharing between provider entities.

## III. LEGAL DISCOVERY RULES

Legal discovery is the means through which evidence is produced for lawsuit purposes from those who have it.[27] The scope of discovery is quite broad. For example, the Federal Rules of Civil Procedure, which govern federal civil lawsuit claims and have been adopted by most states, indicate that parties have the right to any information regarding all matters "relevant" to the case that are not protected by a specific evidentiary privilege.[28] Indeed, discoverable materials and information need not be admissible at trial; they simply need to be "reasonably calculated" to lead to the discovery of admissible information.[29]

---

24. 42 U.S.C. §241(d) (2000).

25. Murphy v. Philip Morris Inc. et al., No. CV997155RAPJWJX, 1999 WL 33521196, at *4 (C.D. Cal. Dec. 28, 1999).

26. Wolpin v. Philip Morris, Inc. et al., 189 F.R.D. 418, 427 (C.D. Cal. 1999).

27. JOSEPH W. GLANNON, CIVIL PROCEDURE: EXAMPLES AND EXPLANATIONS 327-328 (4th ed. 1997). Note that accreditation mandates place providers in precarious positions because they require external reports of systems accidents and failures; these policies do not take into account basic discovery concerns. *See e.g.*, Bryan A. Liang & Kristopher Storti, *Creating Problems as Part of the "Solution": The JCAHO Sentinel Event Policy, Legal Issues, and Patient Safety*, 33 J. HEALTH L. 263, 268 (2000). Such information has been deemed discoverable. *See* Liang, *supra* note 4, at 362 n.29.

28. FED. R. CIV. P. 26(b).

29. *Id.*

Further, the United States Supreme Court has facilitated legal discovery. The Court issued rules on "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.[30]

As applied to patient safety consortium members, absent any privilege protection, reports, and information shared between consortium members and consortium repositories would likely be subject to legal discovery from either. Courts would probably deem such reports and information relevant to a patient injury suit and subject to discovery; this information also would likely be within the automatic disclosure requirements. In addition, such safety information could be seen as reasonably calculated to lead to information that would be admissible at trial.

Certificate of Confidentiality protection under 241(d) would not be helpful to protect consortium information in these circumstances. Any privacy protected under this provision would likely be waived by the patient to allow for its use in the lawsuit.

However, AHRQ 299c-3(c) protection would likely be available to protect safety consortium information, which highlights the importance of this provision. AHRQ protection could act as a specific evidentiary privilege, precluding discovery of shared safety data and information, reporter identities, member reports and consortium member feedback. In this situation, safety communications between consortium members would be protected and facilitate exchange between members. It bears emphasizing; however, that the AHRQ privilege does not preclude traditional material discovery: discovery still reaches materials such as patient charts when requested from individual providers.

### *A. State Privilege Laws*

#### 1. Peer Review/Quality Assurance Privilege (PR/QA)

The IOM Report stated that PR/QA privilege is a promising source of protection for sharing patient safety information among providers.[31] All states adopted some form of PR/QA privilege.[32] The scope of these statutes generally encompasses provider assessment of care delivery and internal quality reviews.[33] However, although potentially helpful in protecting some internal efforts, it is

30. FED. R. CIV. P. 26(a)(1)(B).

31. IOM, *supra* note 1, at 119-121.

32. Susan O. Scheutzow, *State Medical Peer Review: High Cost But No Benefit—Is It Time for a Change?*, 25 AM. J.L. & MED. 7, 9 (1999).

33. *See* Liang, *supra* note 21.

unlikely that PR/QA privilege will protect key consortium information, reporter identities or shared member reports and communications from legal discovery.

First, it should be noted that state PR/QA laws focus upon traditional QA and PR activities.[34] Yet, patient safety research projects arguably would not fall within the standard definition of PR/QA based on PR/QA laws and court holdings.[35] Indeed, safety work often requires investigation into areas and processes that have little to do with direct care activities, including aspects of administrative processes, communication methodologies, standardization practices, technology use and interfaces, and other non-traditional PR/QA functions. In addition, safety work often is deemed "research" rather than quality improvement, which then places it into a different legal domain.[36]

Second, state PR/QA statutes vary tremendously across states. Some of these laws only apply to specific entities (e.g., only hospitals), some focus the profit status of the provider (e.g., they do not include for-profit entities), some extend protections on the basis of managed care status (e.g., they apply only to non-managed care organizations), and, importantly, some do not cover third party entities contracting with a provider to assist in performing QA.[37] This latter circumstance appears to apply directly to outside safety consortium members and repositories collaborating with the provider in safety research, particularly because of the non-traditional focus (at least from a healthcare perspective) of safety investigations and safety improvement activities compared with PR/QA.

Third, courts narrowed the scope of PR protections extensively.[38] This trend is consistent with U.S. Supreme Court jurisprudence that expressly disfavored PR-based discovery limitations;[39] also, it is consonant with other Supreme Court decisions[40] limiting evidentiary privilege.[41]

State courts also are reticent to extend PR/QA privilege too far. First, these courts have found that PR/QA privilege is not absolute: "[i]f the 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."[42] Further, these courts indicated that committees and other subunits of providers

---

34. Liang & Storti, *supra* note 27, at 272.

35. Bryan A. Liang, *Error in Medicine: Legal Impediments to U.S. Reform*, 24 J. HEALTH POL. POL'Y & L. 27 (1999).

36. J. Lynn, *When Does Quality Improvement Count as Research? Human Subject Protection and Theories of Knowledge*, 13 QUALITY & SAFETY HEALTH CARE 67 (2004).

37. Liang, *supra* note 4, at 352.

38. Barry B. Cepelewicz et al., *Recent Developments in Medicine and Law*, 33 TORT & INS. L.J. 583, 588-591 (1998).

39. *See e.g.*, Univ. of Pa. v. EEOC, 493 U.S. 182 (1990).

40. *See* Trammel v. United States, 445 U.S. 40 (1980).

41. United States v. Nixon, 418 U.S. 683 (1974).

42. Sw. Cmty. Health Servs. v. Smith, 755 P.2d 40, 45 (N.M. 1988).

or health care entities must perform traditional PR and QA activities to obtain the benefits of PR/QA privilege;[43] indeed, such activities must be its primary function.[44] State courts additionally emphasized that an entity cannot simply deem any and all members of its staff as part of a "PR/QA Committee" in an effort to extend the privilege broadly.[45]

In addition, important for consortium efforts, state courts also held that disclosure of information gleaned in PR/QA deliberations to third parties[46] may waives the privilege.[47] Further, courts held that one institution's PR/QA privilege does *not* apply to other institutions, and disclosure to third parties expressly waives the privilege.[48] Indeed, even partial PR information disclosure[49] can waive any previously existing privilege.[50]

Finally, it should be noted that PR/QA privilege is state-based. In general, under standard jurisdictional rules, any cause of action involving federal law generally will not be subject to state law privileges, induding PR/QA.[51] Therefore, if a malpractice claim, generally a state law claim, is pleaded with a federal cause of action (e.g., an EMTALA violation, ERISA claim, HIPAA violation, federal antitrust law, federal consumer protection law, federal discrimination law, federal human protection in research law or other federal claim), the federal court may take jurisdiction over the state malpractice claim. In this circumstance, federal evidence and privilege rules apply, thus eliminating any protections of state PR/QA privilege.[52] Such a result is consistent with the federal Health Care Quality Improvement Act, which provides qualified immunity to PR/QA participants but not to any PR/QA materials.[53]

---

43. *See, e.g.*, Freeman et al. v. Piedmont Hosp. et al., 444 S.E.2d 796 (Ga. 1994).

44. *See*, *e.g.*, Claypool v. Mladineo, 724 So. 2d 373 (Miss. 1998).

45. *See*, *e.g.*, Franzen v. Children's Hosp. of Wis., 485 N.W.2d 603, 608 (Wis. Ct. App. 1992).

46. Susan O. Scheutzow & Sylvia Lynn Gillis, *Confidentiality and Privilege of Peer Review Information: More Imagined Than Real*, 7 J.L. & HEALTH 169, 190-92 (1992-93).

47. William D. Bremer, Annotation, *Scope and Extent of Protection from Disclosure of Medical Peer Review Proceedings Relating to Claim in Medical Malpractice Action*, 69 A.L.R.5th 559, 559-624 (1999).

48. *See, e.g.*, Terrell State Hosp. v. Ashworth, 794 S.W.2d 937, 938 (Tex. App. 1990).

49. *See*, *e.g.*, Whitman v. United States, 108 F.R.D. 5 (D.N.H. 1985).

50. *See*, e.g., Thomas C. Riney & Christopher D. Wolek, *Hippocrates Enters the New Millennium—Texas Medical Privileges in the Year 2000*, 41 S. TEX. L. REV. 315, 356-60 (2000).

51. Liang & Storti, *supra* note 27, at 273.

52. *Id.*

53. 42 U.S.C. § 11101-11152 (2000).

2. Attorney-Client Privilege and Work-Product Doctrine

Attorney-client privilege exists to protect communications between attorneys and clients.[54] This allows full candor so the attorney may best advise his/her client in the relevant legal circumstance.[55] Although there were some efforts to protect health care quality information using attorney-client privilege, two major weaknesses of this privilege make it inapplicable to safety information consortium efforts.

First, as with PR/QA privilege, any disclosure of the information to third parties[56] waives the privilege.[57] Hence, as applied to provider safety consortium information sharing, error and data reports by a consortium member will likely waive any possible privilege the member might have outside the institution if dissemination had been limited to its attorney.

Second, and more important to consortium situations, if provider information that should be protected is disclosed or discussed for any reason *other than* in preparation for litigation—such as for safety and consortium purposes—the information becomes discoverable. This results because dissemination then went beyond the traditional parties and purpose of the legal privilege.[58]

Similarly, attorney work-product doctrine protection does not provide consortium information safeguards for its unintended, non-safety improvement use. Work product represents an attorney's preparation for a client's case,[59] i.e., an attorney's litigation strategy. This strategy generally is not discoverable by the opposing party.[60] However, as applied to patient safety data sharing efforts, it is highly unlikely that consortium member reports, repository analysis and feedback, and shared consortium information would be considered an attorney's preparation for litigation. They would not, therefore, be within attorney work product protections.

Furthermore, simply requiring the presence of an attorney during data sharing and information discussion, reporting and assessment is insufficient to invoke work-product protections to the information.[61] In fact, if documents to be protected are created in the normal course of business, they are not considered work product.[62] This latter situation seems to apply to provider consortiums

---

54. Liang, *supra* note 4, at 353.

55. *Id.*

56. *See, e.g.*, Chicago Trust Co. v. Cook County Hosp., 698 N.E.2d 641 (Ill. App. Ct. 1998).

57. *See, e.g.*, State *ex rel.* United Hosp. Ctr., Inc. v. Bedell, 484 S.E.2d 199 (W. Va. 1997).

58. *Id.*

59. Hickman v. Taylor, 329 U.S. 495, 510-511 (1947).

60. *Id.*

61. *See, e.g.*, Wardleigh v. 2nd Jud. Dist. Ct., 891 P.2d 1180 (Nev. 1995).

62. *See, e.g.*, Stout v. Ill. Farmers Ins. Co., 150 F.R.D. 594 (S.D. Ind. 1993), *aff'd*, 852 F. Supp. 704 (S.D. Ind. 1994).

who are regularly participating in patient safety activities, and in light of accreditation mandates that are requiring participation.[63]

## IV. HIPAA MEDICAL PRIVACY PROVISIONS

It is apparent that error reports and data analysis in provider patient safety consortiums would likely disclose and utilize patient information. As such, HIPAA medical privacy provisions and requirements likely would apply to these activities.[64]

HIPAA rules cover all patient-identifiable care "protected health information" ("PHI"),[65] in any form, maintained or transmitted by "covered entities."[66] The latter includes providers, provider contractors and subcontractors and health plans.[67] 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.[68] There are significant requirements for HIPAA covered entities with regard to its business associates. For example, contracts between these parties "must limit business associate's use and/or disclosure of patient information to parties specified" within the agreement;[69] these contracts must mandate "specific security, inspection, and reporting mechanisms" by business associates, *and* by business associate subcontractors.[70] Further, covered entity and business associate internal records must be made available to the Secretary of the Department of Health and Human Services if requested,[71] and "all protected information must be returned or destroyed at the end of the contract period, if practicable."[72] The covered entity may be held responsible for HIPAA rule violations of its business associates if it has knowledge of these violations.[73]

To encourage rule adherence and limited patient information dissemination and use, penalties for HIPAA violations are severe. Both civil monetary penalties

---

63. Bryan A. Liang, *Other People's Money: A Reply to the Joint Commission*, 33 J. HEALTH L. 657, 661-62 (2000).

64. Health Insurance Reform: Security Standards, 68 Fed. Reg. 8334 (Feb. 20, 2003) (to be codified at 45 C.F.R. pts. 160, 162, 164).

65. 45 C.F.R. § 100-103 (2003).

66. *See* Liang, *supra* note 4, at 353. *See also* 45 C.F.R. §§ 160.102, 160.103, 164.500, 164.501 (2003).

67. *See* Liang, *supra* note 4, at 353. *See also* 45 C.F.R. §§ 160.102, 160.103, 164.500, 164.501 (2003).

68. *See* Liang, *supra* note 4, at 354. *See also* 45 C.F.R. § 164.501 (2003).

69. *See* Liang, *supra* note 4, at 354. *See also* 45 C.F.R. § 164.504 (2003).

70. *See* Liang, *supra* note 4, at 354.

71. *See id.*

72. *See id.*

73. *See id.*

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 HIPAA standard violation.[74] In addition, states may impose their own privacy requirements, for HIPAA represents a floor of medical privacy protection; stricter state laws and more severe sanctions are not preempted.[75]

For non-treatment, payment or healthcare operation functions, covered entities that wish to use or disclose PHI for safety improvement efforts generally must obtain HIPAA patient authorization, a quite involved process.[76] Notably, safety activities are not treatment and payment functions, and providers cannot perform independent safety research under the "health-care operation" provision.[77] Although HIPAA regulations indicate that healthcare operations expressly include "quality assessment and improvement," they expressly note that healthcare operations do *not* encompass studies that result in "generalizable knowledge."[78]

Exceptions to the medical privacy rules may be helpful in performing safety work without patient authorization. There are three exceptions to HIPAA patient authorization requirements: health oversight activities, public health activities and research in traditional "clinical trials."[79] However, health oversight and public health exceptions only encompass public or governmental agencies, leaving only research as a possibility for most entities interested in performing patient safety work.[80]

Unfortunately, it is not clear whether the research exception would extend to patient safety activities. 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 work. The rule, however, outlines two mechanisms by which a covered entity can demonstrate meeting the research exception: (1) have 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;'"[81] or, (2) deidentification, i.e., removing nineteen specific patient identifiers from any patients records to be used.[82] This latter provision is most applicable to patient safety consortiums, particularly since the procedure for demonstrating the former is not well defined.[83]

---

74. *See* Liang, *supra* note 4, at 353.
75. *See id.*
76. *See id.* at 353-54.
77. *Id.* at 353-356. *See also* 45 C.F.R. §164.506 (2003).
78. *See* Liang, *supra* note 4, at 355.
79. *See id.* at 355-56. *See also* 45 C.F.R. § 164.512 (2003).
80. *See* Liang, *supra* note 4, at 355-56..
81. *See id.* at 356.
82. *See id.*
83. *See id.* at 356-57.

Accordingly, to avoid the need to obtain authorization from all patients whose information is used or disclosed in safety consortiums, which would be exceedingly labor intensive, and to circumvent potential HIPAA liability, both provider reporter consortium members and the consortium repository acting as 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 at least a business associate of the reporting providers, contractual arrangements between the two must memorialize HIPAA compliance.[84]

## V. THE LEGAL STRUCTURE OF PATIENT SAFETY CONSORTIA

A patient safety consortium, from a pure data sharing and dissemination perspective, takes various forms, and runs the gamut of being an independent, formal legal entity to simply an association of providers who agree to share information to promote safety. However, an individual provider concern that arises beyond substantive safety process improvement is the potential for liability associated with consortium actions, whether they be from the reporter or repository perspective. For example, a critical concern is the liability associated with inappropriate use of PHI that may invoke the severe penalties of HIPAA privacy rules. Consequently, attention to legal structures is important to limit this risk, particularly for consortium repositories who receive the data and disseminate safety information.

There is a spectrum of legal structures through which a consortium may choose to organize and act. These legal structures are represented by three forms: a partnership, an informal nonincorporated entity and a formal corporation structure.

In general, partnerships are legal entities with joint ownership of assets by all partners and individual partner authority to act in the name of and to bind the partnership.[85] Another important and critical characteristic of partnerships is that liability generated by the actions of one partner generally reaches all members of the partnership.[86] In addition, from an organizational perspective, if any individual partner leaves or any new partner enters, the original partnership

---

84. It bears noting that consortiums are more appropriate for these activities than individual providers. There are significant research and identification issues, particularly in rural and community environments, that make aggregate data sharing a less risky legal option. *See* Liang, *supra* note 17, at 43.

85. *See*, *e.g.*, UNIF. PARTNERSHIP ACT, §§ 101(4)(ii)(6), 202, 301, *available at* http://www.law.upenn.edu/bll/ulc/fnact99/1990s/upa97fa.pdf (last visited Dec. 22, 2005).

86. *See*, *e.g.*, Kansallis Fin. Ltd. v. Fern, 659 N.E.2d 731, 735-36 (Mass. 1996) (stating that the partnership may be liable for one partner's actions if they are done within the scope of the partnership or to benefit the partnership).

usually must be dissolved and a new partnership formed for individual members to act within a valid partnership arrangement.[87]

For patient safety consortiums, partnerships are of limited value. At the outset, it is unlikely that any member would accept being bound by the action of another consortium partnership member. Further, the high costs of re-creating a partnership any time a member is added or leaves would be highly inefficient. Moreover, since all partners share in liability personally, any action of the repository or reporter member that violates HIPAA would reflect on all partnership members, which again would likely be unacceptable to any potential safety consortium member.

On the other hand, the unincorporated nonprofit association may be a viable alternative to a partnership. In general, these associations base their 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.[88] 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 under this kind of arrangement would be a matter of the new member agreeing to specified terms orally or in writing. Members who wish to withdraw simply could invoke termination procedures specified by their agreement.

Any potential liability generally focuses upon the discrete individual member and its acts;[89] however, it should be noted that if the association is for-profit, it likely would be considered a partnership with its attendant reflection of liability on all members.[90] Once again, using HIPAA as an example, any liability associated with inappropriate PHI use or disclosure in the non-profit association by, say, a reporting entity and its business associate, would be limited to the individual offending party(ies). Any other member of the association generally would not be implicated by HIPAA liability for the actions of the offending reporter and repository. But an important characteristic should be noted: under this structure, liability is not limited; any and all assets of the offending party(ies) may be reached to satisfy legal penalties.

Because of the latter liability concern, the most protective legal structure for a safety consortium may be a 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 safety information repository, can create the corporation. This entity then may allow other members to affiliate with it, either through purchase of corporate shares or by contract; both approaches allow for simple addition of

---

87. *See*, *e.g.*, Browne v. Ritchey, 559 N.E.2d 808 (Ill. App. Ct. 1990).

88. *See*, *e.g.*, UNIF. UNINCORPORATED NONPROFIT ASS'N. ACT, § 1 Comment 1, *available at* http://www.law.upenn.edu/bll/ulc/fnact99/1990s/uunaa96.txt (last visited Oct. 28, 2005).

89. Heleniak v. Blue Ridge Ins. Co., 557 N.Y.S.2d 229, 230 (N.Y. App. Div. 1990).

90. Shortlidge v. Gutoski, 484 A.2d 1083, 1086 (N.H. 1984).

new members. Assuming that corporate formalities are satisfied (i.e., independent accounting, judgment, and decisionmaking 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) formally may collect safety information, act as a repository, analyze data and communicate lessons back to members. An entity may act as both a member representative (e.g., reporter) and as a corporation representative (e.g., 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 for inappropriate use or disclosure of PHI, only the corporation's assets generally would be reachable for liability purposes.[91] In this case, assets of the individual member acting as the repository cannot be accessed generally.[92] And only if a member reporter has actual knowledge of its business associate repository violation of the HIPAA privacy rules would the individual reporter be subject to HIPAA liability for the repository's actions. Of course, if an individual reporter consortium member violates HIPAA, it can always be reached for liability. However, no other member will share liability in this circumstance, whether the corporation is implicated or not.

## VI. THE PATIENT SAFETY AND QUALITY IMPROVEMENT ACT

As noted above, patient safety activities were thwarted by the vagaries of the legal system. Information and analysis of medical errors, system weaknesses and proactive effort to promote safety can and are subject to legal discovery by attorneys to support their lawsuits. This situation chills any efforts to work in this area, particularly by non-hospital physicians who have virtually no protections for participating in this work.

However, in an effort to address this issue, the Patient Safety and Quality Improvement Act of 2005 became law on July 29, 2005.[93] Under this law, both individual and organizational providers can report voluntarily, share, discuss and formulate information on medical errors and patient safety. The information is confidential and privileged and cannot be used to support non-intended uses of the information, including lawsuits.

---

91. *See, e.g.,* FEC v. Beaumont, 539 U.S. 146, 154 (2003) ("State law grants corporations special advantages...Such as limited liability, perpetual life, and favorable treatment of the accumulation and distribution of assets...") (quoting Austin v. Mich. Chamber of Commerce, 499 U.S. 652, 658-659 (1990).

92. 18B AM. JUR. 2D *Corporations* §§ 1715-31 (2004).

93. Patient Safety and Quality Improvement Act of 2005, Pub. L. No. 109-41, 199 Stat. 424.

### *A. An Overview of the Act*

The Act amends Title IX of the Public Health Service Act[94] to protect a provider's "patient safety work product."[95] This includes data, reports, records, other materials (e.g., root cause analyses), and analyses in oral or written form assembled in a provider's "patient safety evaluation system"—a provider's system created to promote quality and safety in delivery of health care by it. To obtain legal protections, the provider must use information from its patient safety evaluation system and work with a "Patient Safety Organization" ("PSO"), an entity that provides analysis and feedback as to best practices, improvements in care, and other activities that promote quality and safety in health care.[96] The Secretary of the Department of Health and Human Services will certify and register PSOs at a future date, once regulatory explanations are issued.

The statutory protection prohibits patient safety work product from being disclosed or used in any administrative, civil, and criminal proceeding as well as in provider disciplinary proceedings.[97] It also exempts the work product from all state or federal Freedom of Information Act requests.[98] For these voluntary reports, the law's reach is very broad and provides very extensive protection for safety and quality data, yielding significant opportunities to participate in patient safety improvement and promotion.

Note, however, that there are some limitations to the Act's protections. Standard discoverable materials such as the patient's chart, billing records, discharge information, or any other original patient or provider record is not considered patient safety work product and, hence, is not protected by the law.[99] In addition, separately collected or maintained information cannot become patient safety work product merely by submitting it to a PSO.[100]

### *B. Exceptions*

There are some exceptions to privilege and confidentiality; however, they are limited. For example, disclosure of patient safety work product for use in a criminal proceeding is permitted; however, a court must make an *in camera* determination that the work product contains evidence of a criminal act; that it is material; *and,* it is not reasonably available from any other source.[101] Privilege

94. 42 U.S.C. § 299 (2005).
95. 42 U.S.C. § 299b-22 (2005).
96. 42 U.S.C. § 299b-21(4), (6), (7) (2005).
97. 42 U.S.C. § 299b-22(a), (b).
98. § 299b-22(a)(3).
99. § 299b-21(7)(B)(ii).
100. § 299b-22(7)(B)(ii).
101. § 299b-22(c)(1)(A).

and confidentiality of patient safety work product also is disclosable if authorized for disclosure by all providers identified in the work product materials.[102] Deidentified work product disclosure is allowed,[103] as is work product disclosed for FDA-governed products and activities.[104]

It is interesting to note that the statute also allows voluntary disclosure to a provider's accrediting body.[105] However, due to the punitive nature of some accreditors who may use patient safety work product to sanction providers, the Act specifically indicates that providers cannot be forced by an accreditor to reveal its communications with any PSO.[106] Moreover, accrediting bodies cannot take accreditation action against a provider on the basis of provider collection, development, reporting, or maintenance of patient safety work product.[107]

Importantly, the law's protections of the materials travel with the materials themselves[108] rather than being based upon discussion or presence within a specific committee, such as those within a peer review committee. Hence, protections still apply when patient safety work product is transferred to another party. This is a critical provision of the Act because, traditionally, disclosure of privileged information, such as peer review information, to third parties often vitiated any privilege that protected materials might have had before disclosure. This prevented information from being disseminated or discussed by a broad array of providers within an institution and precluded any disclosure outside the institution, forcing each entity to discover safety issues independently.

Finally, the Act does not affect state laws requiring provider reports on non-patient safety work product.[109] This would include, for example, state-mandated nosocomial infection reports or mandated FDA reports.

### *C. Penalties*

For reckless or knowing disclosure of patient safety work product, penalties include civil monetary penalties of up to $10,000 per violation.[110] The statute also protects good faith reporters for wrongful adverse employment actions.[111] If an employer retaliates against persons who report safety information either to the provider or PSO, these persons can bring an equitable civil suit against the

---

102. 42 U.S.C. § 299b - 22(c)(1)(C).
103. § 299b-22(c)(2)(B).
104. § 299b-22(c)(2)(D).
105. § 299b-22(c)(2)(E).
106. § 299b-22(d)(4)(B).
107. 42 U.S.C. § 299b-22(a)(4)(B).
108. § 299b-22(d)(1).
109. 42 U.S.C. § 299b-21(7)(B)(iii)(II).
110. 42 U.S.C. § 299b-22(f)(1).
111. § 299b-22(e)(2).

provider.[112] These equitable suits include orders to stop providers from acting wrongfully against reporters, employment reinstatement, back pay, and benefit restoration.[113]

### *D. HIPAA and PSOs*

HIPAA is specifically addressed by the law. PSOs are treated as provider business associates, and PSO patient safety activities are considered "health care operations" of the provider.[114] Hence, HIPAA authorization from individual patients is not required for patient safety activities.

## VII. RECOMMENDATIONS FOR CREATING PATIENT SAFETY CONSORTIA

Although the Patient Safety and Quality Improvement Act provides great protections and potential for improving patient safety and engaging a larger group of health care providers to participate in this work, issues remain. First, presently there are no regulatory standards nor functioning PSOs. Therefore, no protections of voluntary patient safety activities can be extended yet. Second, some providers may not wish to engage in voluntary reporting of their safety information due to the uncertainty of the legal scope of protections indicated within the Act. Third, there is the significant question as to whether patient safety research, rather than individual quality improvement efforts, will be protected under the statutory provisions; indeed, the question arises as to whether data assembled for more than one purpose that includes patient safety will take the information outside the law's umbrella protections.

Hence, providers may wish to form consortiums in the interim while these important issues are addressed. As such, the traditional legal concerns still attend these efforts. Below, some recommendations are provided with respect to consortium formation for immediate patient safety activities. It should be noted that many of these provisions may still be applicable when PSO regulatory structures and other legal questions are answered.

### *A. Obtain 299c-3(c) Protection*

It appears that AHRQ statutory protection represents the greatest likely source of protection of safety data, reporter identities, and shared information discussed between consortium repositories and members. Further, the AHRQ confidentiality provision also addresses the potential liability concern that even if patient PHI is appropriately deidentified under HIPAA, the consortium

112. 42 U.S.C. § 299b-22(f)(4).
113. § 299b-22(e), (f)(4).
114. § 299b-22(i).

member reporter still might be identifiable. Since 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 such as to support lawsuits.[115] Accordingly, deidentification of patient data information that fulfills the HIPAA privacy rule will likely not vitiate AHRQ protections for the provider reporter. Further, 299c-3(c) protection likely would be considered a privilege against discovery under civil procedure rules, which also may preclude attorney efforts to obtain data or the results of analyses to support lawsuits, which has been attempted in the past.[116] However, it should be emphasized that 299c-3(c) protection will not preclude discovery of traditionally discoverable materials such as the patient's chart.

### *B. Seek Out State-Specific Privileges*

Although unlikely to provide comprehensive protections of safety consortium exchange information, state-specific PR/QA and similar privileges may offer some protections through that particular state's law and the consortium's unique circumstance.

State PR/QA laws specifically may protect sharing of safety data between regional or state-wide institutions. For example, in California, trauma care under Evidence Code § 1157.7 is carved out in this manner,[117] facilitating the creation of regional trauma networks and substantial improvements in trauma care through sharing of patient outcomes and quality improvement strategies. In other jurisdictions,[118] there are state-specific discovery protections for patient safety data.[119]

### *C. 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 or disclosure, HIPAA deidentification requirements should be adhered to in consortium information transfer and sharing. Such deidentification under the privacy rule likely will not eliminate AHRQ 299c-3(c) protections. It is equally important to deidentify provider and institution identities in data submitted to the consortium repository or shared among consortium members; such deidentification may provide an additional barrier to ensure that safety information is limited to its intended use.

---

115. 42 U.S.C. § 299c-3(2005).

116. Bert Black, *Subpoenas and Science—When Lawyers Force Their Way into the Laboratory*, 336 NEW ENG. J. MED. 725, 725 (1997).

117. CAL. EVID. CODE § 1157.7 (West 1995).

118. *See*, *e.g.*, VA. CODE. ANN. § 8.01-581.17 (Lexis 2002).

119. *See*, *e.g.*, FLA. STAT. ANN. § 766.101 (West 2003).

### *D. The Consortium Should Create A Legal Structure.*

Consortium members and, in particular, members acting as a repository, should carefully consider specific legal structure under which they wish to operate. The corporation is likely the most effective structure to limit liability and protect assets of any member acting as the repository of safety information. Unincorporated associations using member contracts may be an acceptable alternative; however, they suffer from the concern that liability is not limited. Like confidentiality provisions under AHRQ, it should be noted that no legal structure will prevent a plaintiff from suing an individual provider and obtaining standard discoverable information.

## VIII. POLICY REQUIREMENTS

To promote patient safety most effectively, rapidly, and proactively, it is apparent that institutions must share information. More deeply, there must be a cultural acceptance and promotion of institutional accountability and individual provider acceptance and competency in team based approaches and coordinated action.

Of course, critically, as the IOM Report recommended, federal legislation must be enacted so it is clear to individual and institutional providers that reporting system weaknesses and errors and sharing information is to be rewarded, not punished. Legislation such as the Patient Safety and Quality Improvement Act is ideal for such efforts, but as noted previously, its provisions raise some unanswered questions for practical use. In the interim, creation of numerous consortiums could become a reality and standard in improving health care safety and quality and could be the basis of a new integrated system of data sharing in concert with the provisions of the Act.

But legal reform, while a necessary condition, is not sufficient. The varying competitive forces for the health care dollar in the compliance arena require that providers consider whether to allocate resources to patient safety or to other mandated areas such as fraud and abuse, the latter of which have significant civil and criminal penalties whereas the former has less obvious downside costs—at least on the short term bottom line.

Indeed, because of the importance of legal protections under AHRQ 299c-3(c) and the need to provide some financial assistance to providers, greater funding of patient safety research, perhaps in smaller amounts, to a broader array of providers, would create incentives for a larger number of providers to participate in data sharing to improve safety in their delivery systems. Instead of Agency grant efforts focused on a particular area or on one grantee such as recent requests for applications[120] accomplished, a more proactive approach would be

120. *See, e.g.*, AHRQ, *State and Regional Demonstrations in Health Information Technology: Request for*

one that promotes consortium formation and activities with mechanisms for dissemination of results from these laboratories of safety learning. It is particularly important to bring the safety concepts, knowledge and learning to the outpatient setting which is traditionally ignored in the patient safety world. The new Patient Safety and Quality Improvement Act extends its protections to this delivery venue, and support must be found to engage its members.

As a societal matter, to support safety efforts, a significant shift away from the individual orientation and towards system-based accountability in both law and medicine must occur.[121] Complex systems require broad-based, institutionally oriented ethical approaches that do not assume linear cause-and-effect processes. Instead, the multifaceted and compound interactions and realities must be accepted and form the basis of how an entity within a complicated functional network can move forward in promoting safety.[122] Instead of believing that a single individual within an entity is only responsible for a single aspect of care, the focus should be on a group ethic of prevention of harm to the patient through transparent information flow, within and across the system.[123] Those who report on system weaknesses and make transparent error processes should be rewarded, not punished, as both the current legal and medical systems do.[124] Such an approach actually expands the ethical duties of individual members of an organization and serves to promote actions that, again, focus on preventing harm, ensuring systems can absorb inevitable human error, and encouraging lessons to be shared.[125]

Although a robust culture change is needed to fundamentally promote such organizational efforts, medical education is clearly implicated as well by the need to openly share information and data on safety experience within and outside institutions. In particular, students in the health professions must be trained in the tools of systems analysis, clear communication methods, blame-free efforts to promote quality and safety, and team approaches to error analysis and resilient systems design. Then they will be primed to participate fully and effectively in safety consortium efforts. However, leaders in medical education must reject

---

*Proposals*, http://www.ahrq.gov/fund/contarchive/rfp040015.htm (last visited Dec. 22, 2005).

121. Bryan A. Liang, *A Policy of System Safety: Shifting the Medical and Legal Paradigms to Effectively Address Error in Medicine*, 5 HARV. HEALTH POL'Y REV. 6, 10-12 (2004).

122. Bryan A. Liang & LiLan Ren, *Medical Liability Insurance and Damage Caps: Getting Beyond Band Aids to Substantive Systems Treatment to Improve Quality and Safety in Healthcare*, 30 AM. J.L. & MED. 501, 523 n. 214 (2004) (describing the complexities of "white spaces" in organizations that must be addressed to promote safety).

123. Liang, *supra* note 121, at 11.

124. *See id.* at 9.

125. *See id.* at 11-12. Note, however, sometimes these kinds of efforts result in focusing upon individuals to ensure and promote system safety. The key difference in this latter approach compared with the traditional individually-oriented shame and blame approach is that the goal is corrective action for system outcomes; not individual punishment based on fear.

their traditional "gentlemanly honor" culture;[126] they must retrain to adopt the modern safety principles so they can ensure the next generation of providers is equipped to implement the systematic efforts that require team approaches, transparent communications, and sharing of data to improve patient safety.[127]

## IV. CONCLUSION

To promote patient safety, sharing information on errors, system weaknesses, and successful approaches are key. Patient safety consortiums can, therefore, be a powerful and positive force in that process. There may be legal methods to address these issues, such as the use of AHRQ protections, and other legal approaches such as the newly enacted Patient Safety and Quality Improvement Act. Yet, legal reform alone is not enough. A shift to embrace institutional ethics and educational reform to ensure providers have relevant system and team tools to improve system safety is necessary for lasting change. Otherwise, we leave for yet another generation an inefficient, punitive legal and medical system that simply points fingers while sacrificing the safety of patients in our health care delivery system.

---

126. The "gentlemanly honor" paradigm of physician accountability is the traditional medical ethic focused upon the individual provider being responsible for any untoward outcome of a patient as well as taking full credit for any benefit the patient receives. *See* Virginia A. Sharpe, *Behind Closed Doors: Accountability and Responsibility in Patient Care*, 25 J. MED. PHIL. 28, 29-30 (2000). Such an approach is wholly inconsistent with modern medical care delivery. *See* Liang, *supra* note 121, at 9-10.

127. Laura Lin & Bryan A. Liang, *Reforming Residency: Modernizing Resident Education and Training to Promote Quality and Safety in Health Care*, 38 J. HEALTH L. 203 (2005). Indeed, human factors approaches recognizing the human condition must guide training efforts to safeguard safety and provide a sound foundation for medical care delivery rather than the haphazard methods currently extant.