E-Briefings

VOLUME 21 • NO. 6 • NOVEMBER 2024

The Governance Institute

What's Inside:

All or Nothing: Shaping Healthcare's Role in Social Determinants of Health

By David Jarrard, Chairman of *Jarrard Inc. Executive Committee*

If everything is healthcare, then nothing is.

The conservative Manhattan Institute think tank argued this summer that the "non-medical factors" used by the federal government to address the social determinants of health (SDOH) have led to "unjustifiable" increases in public and healthcare organizations' spending on housing, education, food, and neighborhood environments.[1]

"Is everything healthcare?" the author asks. "The best-designed experiments with randomized controlled trials—the gold standard of social science research—typically find that SDOH expenditures have weak effects on health and few offsetting savings."

Of course, there's little doubt better nutrition, better education, and other societal goods are deeply associated with better health—and better healthcare outcomes—for people who receive them, even if the line linking the two in some research is more dotted than solid.

But "if everything is healthcare," how are mission-minded but fiscally responsible health system leaders to allocate their organization's resources? Clearly, they can't do everything. For a health system to fully address every potential SDOH in their community would bankrupt it.

This is not a dismissible academic exercise with no practical consequence for health system leaders.

1 Chris Pope, "Is Everything Health Care? The Overblown Social Determinants of Health," Manhattan Institute, July 11, 2024.

The Institute's essay—and the feedback that followed—are the latest salvos in today's energetic and consequential discussion about whether and how health systems are helping their communities beyond the walls of their exam rooms.

The Lown Institute regularly asks whether non-profit hospitals do their "fair share" and thereby earn (or fail to earn) their tax exemptions.[2] Others, such as Johns Hopkins professor Marty Makary, M.D., are more prescriptive: hospitals that generate "profits" and do not use those excess dollars to fund charity services should pay taxes on it.[3]

It's part of a larger national conversation about the delivery of care in the U.S. Who delivers it? Who pays for it? Who determines its value? What should the public (and taxpayers) fairly expect from health systems now? Is the public getting "enough"—however that's defined—for its healthcare dollar?

Behind these questions, proposals for tightening regulations on community benefits and hospital tax exemptions follow closely, with growing public support

But questions are also opportunities. Honest questions form a table for discussion, for listening, and for the pursuit of shared understanding. Health systems leaders would do well to welcome and join the roundtable that is occurring now with or without their voices.

Below are three ways healthcare boards and senior leaders can—and should—impact this important debate.

Declare Your Healthcare Corner

Your organization can't do everything that could encompass healthcare delivery (and none can). But it can do select things very well. Do those things, fearlessly.

Boldly own that niche of healthcare delivery in which your organization can make a discernable difference, in which it can excel, and in which it invests its blood and treasure in pursuit of its mission.

For your organization, this may be dramatic commitment to a service line, such as cancer treatment or cardiology care. It may be to an issue, such as a reduction in gun violence or teenage pregnancy or adult obesity in your communities. It may be to offer extraordinary access to care to every neighbor. Whatever is right for your organization and community, own it deeply—and loudly.

Your organization can't do everything that could encompass healthcare delivery (and none can). But it can do select things very well. Do those things, fearlessly.

2 https://lownhospitalsindex.org.

3 Marty Makary, "Hospitals That Make Profits Should Pay Taxes," *STAT*, April 14, 2024.

This strategic focus offers health system leaders many important advantages. Here are two: It allows you to say "no" to many good things so you can say "yes" to a few great things. And it unlocks the power of paying attention.

What's more, this approach engages the question "Is everything healthcare?" by modeling how smart systems can participate in the answer without having to be **the entire solution to it.** Your deliberate focus sets the stage for answers that can only come from a community of providers in partnership.

Key Board Questions

Start the conversation in your next board meeting with these prompts:

- Are we trying to be everything to everybody, or do we have select focus areas that differentiate us in the market?
- Do we know all the individuals, groups, and organizations that comprise the full spectrum of healthcare in our market?
- Do we have relationships with and are we working with those individuals, groups, and organizations?
- What do the opinion leaders in our community (including our legislative delegation) truly know about the community benefits our organization provides?

Convene the Broader Conversation

Use your market strength and goodwill to facilitate conversations among the sweeping ecosystem of organizations working to deliver care in your community—traditional providers, payers, public health players, and more. Once aligned as healthcare providers, bring in the expanded universe of SDOH organizations who address housing, food, and transportation challenges for patients.

Use your organization's gravity to pull together those many voices to an ongoing roundtable. The group itself is a step to defining the "everything" of healthcare. The group is a manifestation of the story you need to tell; healthcare requires a community of care.

> Use your organization's voice to define healthcare delivery—what it is and what it can be—in your community. Most critically, act on your words. Do the part.

Tell Your Organization's Story

Healthcare is in a season of redefinition. Maybe it always is, to some degree. But today's defining conversation has many new voices, including those offering unbalanced critiques of providers and the care they do (or do not) offer. Left unanswered, these voices will have outsized influence over the direction of policy and regulatory initiatives that do not support today's providers.

Assume your community knows little of what your organization does to advance health and well-being beyond your doors. In fact, our surveys show they know very little of what their local health systems do beyond traditional care. But here's the good news: the more they learn, the more their support grows.

Use your organization's voice to define healthcare delivery—what it is and what it can be—in your community. Most critically, act on your words. Do the part.

Is everything healthcare? It's not an idle question. The answer is consequential.

No one is more trusted by the public to answer the question than local healthcare leaders and clinicians. Leverage that trust now. Be part of the answer.

TGI thanks David Jarrard, Chairman, Jarrard Inc. Executive Committee, for contributing this article. David can be reached at djarrard@jarrardinc.com.

Cyber Safety Is Patient Safety

By Greg Garcia, Executive Director, *Health Sector Coordinating Council Cybersecurity Working Group*

Today's healthcare board members must be more aware of and accountable for the cybersecurity of their enterprise than ever before. The healthcare system has seen promising advances in the evolution of digital health, hospital-at-home care, and wearable and implantable devices offering more consumer awareness and control about their health. But with that technological interconnectedness of health data and imaging, shared diagnoses, and remote healthcare is peril: every digital connection is a potential opening for cyber attack.

Hitting Where It Hurts

Data breaches tracked by HIPAA enforcement nearly doubled since 2018 to 725 in 2023, an average of two per day nationwide.[1] Ransomware attacks—which lock up data, systems, and hospital operations that can only be unlocked and returned with the payment of a heavy ransom—hit 141 hospitals in 2023 with an average ransom payment of $1.5 million.[2] The practical impact of this scourge can be catastrophic:

- Disruption or corruption of imaging and other diagnostic and therapeutic devices
- Loss of patient medical records
- Payment systems and scheduling shut down
- Loss and corruption of clinical trial and research data
- Disruption of pharmaceutical manufacturing operations and prescription fulfillment
- Diversion of ambulances and suspension or cancellation of patient care, causing patient harm

Healthcare is now targeted by cyber hackers more than any of the 16 other critical infrastructure industry sectors—more than financial services, communications, transportation, water, chemicals, and many more.

Consider the typical profile of a hospital and its many medical devices and associated cyber-attack risks:

- A patient bed has an average of 15 medical devices.
- A 500-bed hospital could have 7,500 devices, most of which connect to the hospital network.

1 Steve Alder, "Healthcare Data Breach Statistics," *The HIPAA Journal*, September 24, 2024.

2 Steve Alder, "At Least 141 Hospitals Directly Affected by Ransomware Attacks in 2023," *The HIPAA Journal*, January 2, 2024.

- Many fleets of devices are older, legacy devices with operating systems and other software programs that no longer receive maintenance or security patches from the component vendor.
- They often have common passwords set by the manufacturer that cannot be changed.
- Time and cost to update these devices is very expensive.

While cyber attacks have not historically impacted medical devices, they occasionally serve as the portal through which hackers penetrate the wider hospital network and databases, and the cost and complexity of keeping those devices updated—or the risk of not doing so—can be high.

Downstream Risks

Even if your organization is not directly targeted and victimized by a cyber target, it can still experience downstream effects. A study published in the *JAMA Network Open* examined the consequences of ransomware attacks on emergency departments.[3] The study found that an attack on one hospital in Southern California had cascading effects, resulting in increases in patient volumes at adjacent hospital emergency rooms and patients who left without receiving medical attention. The initial attack disrupted electronic health records and imaging systems, forcing clinical staff to revert to using paper records, as emergency rooms diverted patients. Patient health and safety suffered, as evidenced by the 74.6 percent rise in stroke code activations and the 113.6 percent increase in confirmed strokes during the attack phase of the cyber incident. Operations were disrupted for weeks following the attack.

Although ransomware is a threat to all healthcare delivery organizations, those serving rural areas are especially vulnerable due to resource constraints, both for preparation and for response and recovery. About one-fifth of the U.S. population live in rural areas, yet these communities face difficulties attracting cybersecurity talent and obtaining adequate funding for the many demands on clinical and administrative operations. Rural healthcare delivery organizations often depend on unsupported legacy software and hardware, making it challenging to harden these systems.

Enterprise Risk Imperative

Cyber threats are a shared challenge across the enterprise and therefore a shared responsibility. Cybersecurity is ultimately about patient safety, and just as every hospital and health system must consider the following risk categories in the context

> Healthcare is now targeted by cyber hackers more than any of the 16 other critical infrastructure industry sectors—more than financial services, communications, transportation, water, chemicals, and many more.

3 Christian Dameff, et al., "Ransomware Attack Associated with Disruptions at Adjacent Emergency Departments in the U.S.," *JAMA Network Open*, May 8, 2023.

of the ability to continue to provide patient care, cybersecurity must be included as a part—and indeed a controlling factor—of enterprise risk:

- **Clinical/patient safety:**
  - Delayed or disrupted care
  - Corrupted patient data
  - Corrupted diagnostic information
- **Operational:**
  - Downtime
  - Administrative functions like scheduling and billing
  - Facilities disruption of connected utilities such as elevator, HVAC, pharmaceutical refrigeration
- **Financial:**
  - Ransomware expense
  - Recovery costs
  - Legal liability
  - Regulatory fines
  - Stock price impact
- **Reputational:**
  - Crisis communications credibility
  - Loss of patient trust
  - Employee morale
- **Data loss:**
  - Research and clinical trials
  - Intellectual property
  - Protected health information

Pay Now *and* Pay Later

Conventional wisdom holds that it is not *if* your organization will suffer a cyber attack but *when*. Even if you are among the lucky that do not experience a cyber incident, good risk management directs you to invest in both foundational security controls to reduce the risk and severity of impact, as well as in exercises, incident response, backups, and operational continuity to be ready when it does it happen. Paying later also means that, through regulation and legislation, the government will be demanding more of healthcare delivery organizations, as well as the third-party technology and service providers supporting them. This naturally comes at a cost.

As of this writing, the U.S. Department of Health and Human Services (HHS) is readying a slate of regulatory initiatives requiring minimum cybersecurity controls in the health sector. Early in 2024, HHS promulgated these minimum expectations as voluntary "Cyber Performance Goals," which includes 10 "essential" goals that form the foundation of a cyber risk program, followed by 10 "enhanced" goals that should build on those essentials.[4] The essential controls include:

1. Mitigate known vulnerabilities
2. Email security
3. Multifactor authentication
4. Basic cybersecurity training
5. Strong encryption
6. Revoke expired credentials
7. Incident planning and response
8. Unique credentials
9. Separate user and privileged accounts
10. Vendor/supplier cybersecurity requirements

These Cyber Performance Goals are likely to serve as the foundational reference for the regulations, which would use a combination of HIPAA security rule updates and CMS reimbursement linkage as enforcement leverage. For underserved providers, the HHS program and recent supporting congressional bills (which have little prospect of passage in an election year) would provide financial and other technical support to ensure their compliance with these new regulatory requirements.

Conventional wisdom holds that it is not if your organization will suffer a cyber attack but when.

Get Help

The Health Sector Coordinating Council (HSCC) Cybersecurity Working Group (CWG),[5] a health industry council of almost 450 organizations across the health industry that advises the government and the sector on necessary critical cybersecurity policy programs, has been working with HHS and the Congress to consider the most effective approach to strengthening the health sector against cyber threats, while minimizing the additional cost burden that must be balanced against necessary clinical resources.

Government regulation should set baseline expectations ("the what") while industry owners and operators like the membership of the HSCC can share leading practices for "the how," which take into account evolving threats, technology innovation, and business models for flexible and effective cyber risk management programs. Accordingly, to supplement government regulation or to fill in the gaps,

4 HHS, "HPH Cybersecurity Performance Goals."

5 See https://healthsectorcouncil.org.

the HSCC CWG has developed a wealth of voluntary cybersecurity best practices, recommendations, and other free resources,[6] by the sector for the sector, for how to fortify cyber risk management programs. These include hospital cybersecurity leading practices, workforce training and incident response, medical device cybersecurity maintenance and third-party cyber risk management, among many others.

To join and participate in our work or stay up to date with developments in healthcare cybersecurity, visit HealthSectorCouncil.org.

And remember ***cyber safety is patient safety***.

Key Board Takeaways

Five Key Principles for Enterprise Cyber Risk Oversight:

1. Approach cybersecurity as an enterprise-wide risk management issue.
2. Assess legal, financial, reputational, operational, and clinical implications of cyber risks: cyber security mitigates these risks; cyber vulnerability increases them.
3. Set an expectation for management to establish a cyber enterprise risk management framework.
4. Engage external expertise and stakeholder communities for situational awareness.
5. Board/management discussions about cyber risk should include:
    - Identification of which risks to avoid, accept, mitigate, or transfer through insurance.
    - Specific plans associated with each approach.

TGI thanks Greg Garcia, Executive Director of the Health Sector Coordinating Council Cybersecurity Working Group, for contributing this article. Greg also served as the nation's first Assistant Secretary for Cybersecurity with the U.S. Department of Homeland Security from 2006–2009. He can be reached at greg.garcia@healthsectorcouncil.org.

6 See https://healthsectorcouncil.org/hscc-publications.

Medical Staff Peer Review in a Fair and Just Culture: Navigating the Tension

By Daniel Hyman, M.D., M.M.M., Chief Safety and Quality Officer, *Children's Hospital of Philadelphia*

Our committee members sat at a long rectangular table in an otherwise non-descript conference room. Eight or 10 physicians and advanced practice providers would gather around the table, along with staff to our peer review committee. The clinician "invited" to the committee for discussion would be escorted into the room and would sit near the chairperson. Given the inherent nature and potential consequences of the peer review process, it is easy to imagine and understand the anxiety anyone would feel when required to participate. No matter how supportive, collaborative, friendly, and welcoming we may have tried to be, the inherent nature and structure of the peer review meetings at the time could never have fully accomplished the fair and just culture we intended, or the clinician well-being we desired.

I reflect on this prior approach to medical staff peer review (in a previous organization) with a good deal of regret. It wasn't that we had the wrong philosophy or that we were particularly blaming in our discussions. In fact, our stated intent was to be helpful to clinicians having performance gaps in an effort to address them and empathetic with those involved in serious safety events where provider actions were deemed contributory to the event. Rather, my regret is that we didn't recognize that even with a belief in the importance of fair and just culture, our processes needed to more intentionally prioritize clinician well-being while simultaneously seeking to understand and address whatever the issues were that required our colleague to participate in the peer review process in the first place.

As I think about those experiences—for both the involved providers and our committee members—I recognize that the competing needs of robust peer review, fair and just culture, and clinician well-being are, to some extent, in conflict with one another, and that conflict needs to be actively managed. How might we navigate these inherent tensions? Can we accomplish all of them? I think we can, at least in part.

This article offers some potential approaches to reconciling the inherent tensions between the application of fair and just culture in the setting of peer review processes with the goal of promoting clinician well-being.

Fair and Just Approaches to Peer Review

The Joint Commission, state medical boards, Congress, and others have required hospitals, through their medical staffs, to establish peer review processes since the 1950s.[1] Peer review processes are designed to promote the delivery of high-quality patient care and professionalism, and when conducted effectively provide protections to patients, providers, and hospitals alike. Unfortunately, the history of peer review is checkered with examples of punitive processes and cases, and the targeting of physicians due to economic competition that resulted in lawsuits and judgements against hospitals and medical staff members who participated. Case law and subsequent legislation now inform the manner in which peer review must be conducted in order for hospitals and participating physicians to have immunity from claims related to decisions and actions based on peer review processes. The 1986 Healthcare Quality Improvement Act stipulates that physicians (and hospitals) participating in the peer review process will have immunity from civil litigation for their involvement as long as actions are taken to improve quality of care, and after reasonable attempts to gather the facts, so long as the provider received adequate notice and hearing, and the organization had reasonable belief that its peer review action was warranted.[2]

The effectiveness of peer review at addressing performance gaps is uneven. Physicians individually and medical staffs as a whole are not necessarily inclined or good at thinking critically of and disciplining colleagues related to their performance. While it is certainly uncomfortable, we are nonetheless obliged to do so to meet our responsibilities to the hospital, the board, and most importantly, the communities we serve.

It has been 20 years since Dr. Lucian Leape famously said, "The single greatest impediment to error prevention in the medical industry is that we punish people for making mistakes." Since then, we have been encouraged to incorporate principles of fair and just culture into our organizations. How might we think about the tensions between not punishing people for their mistakes, but also upholding the requirements for peer review to ensure high-quality care and professionalism in our hospitals?

1 Robert Wachter and Peter Pronovost, "Balancing 'No Blame' with Accountability in Patient Safety," *New England Journal of Medicine*, October 2009; John Marren, G. Landon Feazell, and Michael Paddock, "The Hospital Board at Risk and the Need to Restructure the Relationship with the Medical Staff: Bylaws, Peer Review, and Related Solutions," *Annals of Health Law*, 2003; Philip Merkel, "Physicians Policing Physicians: The Development of Medical Staff Peer Review Law at California Hospitals," *University of San Francisco Law Review*, 2004; Dinesh Vyas and Ahmed Hozain, "Clinical Peer Review in the United States: History, Legal Development, and Subsequent Abuse," *World Journal of Gastroenterology*, June 2014; Bulletin of the American College of Surgeons, Vol. 85, No. 6, June 2000, p. 24.

2 Vyas and Hozain, June 2014; Bulletin of the American College of Surgeons, June 2000.

I believe it is possible to do so through transparency, consistency, and a systematic approach to evaluations and actions.

Promoting fair and just culture in our organizations starts with leaders having an understanding of the nature of human error and the contribution of systems to the results we achieve. In the words of Dartmouth's Dr. Paul Batalden, "Every system is perfectly designed to get the results it gets." It is our job as leaders to address errors that occur and harm, or could harm, patients and to address gaps in individual performance. We do this best when we start from a place of respect and with an assumption that each individual is well intended, competent, and caring. It is our job to figure out how to help them improve in the context of the system in which they are working. This does not mean there is not individual accountability—to the contrary. Our approach is not called "non-punitive" or "blame free." It is called fair and just to reflect the fact that our intent is to respond to each situation systematically and with consideration of the factors contributing to any clinician's current performance or to their contribution to a significant safety event.[3] No matter how empathetic we may try to be, it is critical to also recognize that any provider is likely to be experiencing some fear, embarrassment, or anxiety when their performance, decision making, or judgement are being questioned. Given that peer review can have consequences for a provider's job status, privileging, or credentialing, leaders and peer review committees must be consistent, transparent, and clear about their approach. They must demonstrate empathy in their words and in their processes. These principles are critical to the experience the provider will have going through the peer review process.

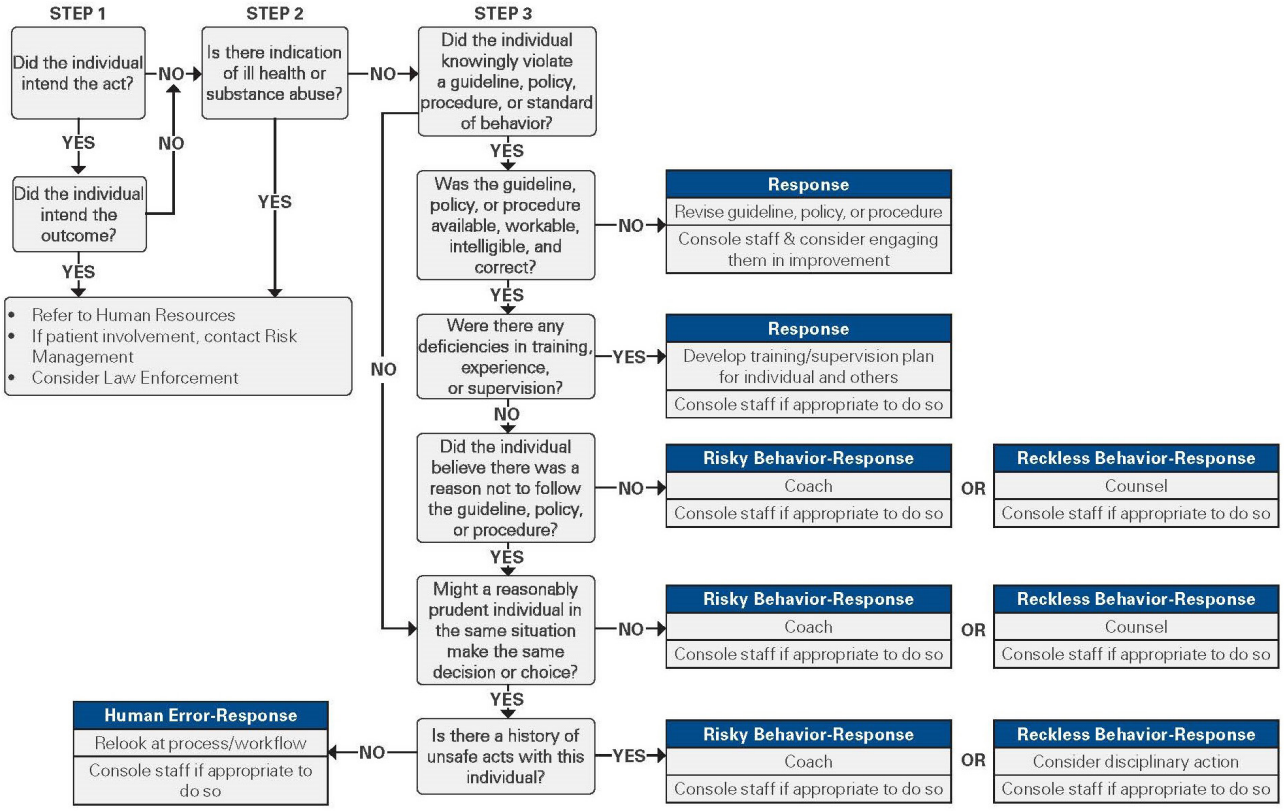
It is our job as leaders to address errors that occur and harm, or could harm, patients and to address gaps in individual performance.

A Just Culture Framework

There are a number of constructs and algorithms leaders can incorporate into their peer review activity when evaluating a provider for an error or other action contributing to a significant safety event. "Just culture" algorithms like the one below can guide the systematic peer review evaluation of clinicians related to adverse occurrences. A similar simplified framework distinguishes normal human error (slips/lapses) from risk-taking and reckless behaviors, and it guides the response that should occur based on the nature of the error. The framework only recommends discipline in the case of reckless or repeated risk-taking behaviors that persist despite coaching.

3 Wachter and Pronovost, October 2009; Allan Frankel, Michael Leonard, and Charles Denham, "Fair and Just Culture, Team Behavior, and Leadership Engagement: The Tools to Achieve High Reliability," *Health Services Research*, August 2006.

Just Culture Algorithm



Based on James Reason's Culpability Model and The NHS Confederation.

Human Error	At-Risk Behavior	Reckless Behavior
• Inadvertent action • Unintentional deviation • Slip • Lapse • Mistake	• Behavioral choice that increases risk • Risk is not recognized or is believed to be justified	• Choice to consciously disregard a rule or standard • Creates substantial and unjustifiable risk
• Coach/seek to learn how system may have contributed to or enabled the error.	• Coach: consider system contributions to the reasons for the behavior.	• Discipline is appropriate for reckless behaviors irrespective of the impact on patients.

Key Board Takeaways

- Board members should inquire as to the nature and function of their medical staff's peer review processes.
- Specific areas of inquiry need to include the frequency that cases are referred to the peer review committee and how they are evaluated and adjudicated.
- Cases appropriately referred for peer review include concerns about professionalism as well as clinical performance.
- Medical staff leadership should ensure that peer review is conducted consistent with the requirements of the Health Care Quality Improvement Act and in accordance with the principles of just and fair culture.

It is appropriate to console clinicians involved in adverse events where their errors would be considered a slip, lapse, or simple human error. We also should seek to learn with each of these opportunities how the system may not have prevented, or potentially even enabled, the error or inappropriate behavior.

As I think back on some of my earlier experiences with peer review processes, I recognize that we had the opportunity to be more transparent about our approach, more systematic in the application of an agreed-upon algorithm, and more empathetic to the people involved by narrowing the group with whom they needed to directly interact to just a few representatives. By approaching peer review in this way, we can ensure the necessary robustness of the peer review process while also supporting our colleagues and treating them in ways that are fair and just and supportive of their personal well-being.

TGI thanks Daniel Hyman, M.D., M.M.M., Chief Safety and Quality Officer, Children's Hospital of Philadelphia, for contributing this article. He can be reached at danhyman2@gmail.com.