

PRACTICE RESOURCE

Is Your Organization Ready for a High-Profile Patient?

Ann G. Taylor, B. Moses Vargas, Jennifer Stevens

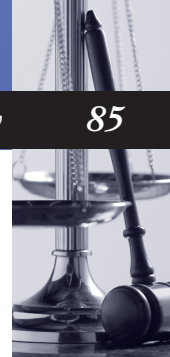
What is the issue? When a hospital is entrusted with providing medical care to a high-profile patient, or when an incident regarding the care of a patient attains high-profile status, the entire organization can become vulnerable to a host of staffing, public relation, and operational issues.

What is at stake? If a hospital does not have in place policies and procedures that key stakeholders involved in the patient's care can rely on, the unique challenges brought on by high-profile patient situations can result in public relation debacles, breach of patient confidentiality, attacks on the organization's operational systems, and an unsafe or confusing work environment for clinicians.

What should attorneys do? Attorneys can equip hospitals to handle high-profile patient scenarios by ensuring that clear policies and protocols are in place and followed by the key stakeholders—and their staff—who are most involved in caring for the patient.

CITATION: Ann G. Taylor, B. Moses Vargas, and Jennifer Stevens, *Is Your Organization Ready for a High-Profile Patient?*, J. HEALTH & LIFE SCI. L., June 2016 at 85. © American Health Lawyers Association, www.healthlawyers.org/journal. All rights reserved.

Author biographies appear on the next page.



[Ann G. Taylor](#) is Executive Vice President and Chief Administrative Officer at Connecticut Children's Medical Center. Contact her via email at ataylor@ccmckids.org.

[B. Moses Vargas](#) is General Counsel at Connecticut Children's Medical Center. Contact him via email at mvargas@ccmckids.org.

[Jennifer Stevens](#) is a law student, Class of 2016, at the University of Connecticut School of Law. Contact her via email at JStevens03@connecticutchildrens.org.

Taylor, Vargas, and Stevens: The High-Profile Patient

CONTENTS

Introduction.....	88
Why Put Legal in the Lead?	89
The High-Profile Patient with a Low Profile	90
Identify key stakeholders and their roles.....	90
Table 1 General Awareness Group.....	91
Table 2 Key Stakeholders.....	93
Frequency of meetings.....	97
The Patient Who Attracts the Media	97
Working with the media	98
Preparing for IT threats.....	100
Working with public officials.....	101
Key Policy Points to Consider in High-Profile Cases	102
Conclusion	106

Introduction

Health care lawyers are privileged to practice in the midst of providers who care for the sick and injured and help families deal with sometimes devastating circumstances. These situations are made more complex when the patient is a “high-profile” patient—either because he or she is a celebrity or because the particulars of his or her case attract public attention. A host of concerns must be addressed, from maintaining confidentiality to managing physical and information security risks created by the attention. The ultimate goals are to do what is right for the patient, ensure the best possible care, and protect the organization and individuals who provide that care. Therefore, it is critical to be prepared.

In this Practice Resource, we will share lessons learned from treating high profile patients and/or dealing with a high-profile incident, and examine the additional planning and resources that became necessary when such cases attracted public attention.

In each type of high-profile patient scenario, nearly every area of our institution—Connecticut Children’s Medical Center (Connecticut Children’s)—was impacted in one way or another. For example, Security, Risk Management, and Facilities staff ensured that employees were safe and the workings of the hospital continued uninterrupted. Public Relations and Corporate Communications spent an enormous amount of time managing the internal and external messages necessitated by each situation. We faced serious information technology (IT) concerns when unusual activity was discovered in our systems. Billing, Coding, and Health Information Management staff implemented additional processes and safeguards to ensure that confidentiality was maintained. There was also extensive coordination with outside agencies such as the local police and the Department of Children and Families. The need to coordinate with these departments and many others will be discussed in more detail below.

Why Put Legal in the Lead?

It is the responsibility of legal counsel to serve as a trusted resource that will keep the institution from violating laws or regulations, ask the right questions, pay attention to detail, and act as the first line of defense for the hospital.

In each of the high-profile patient scenarios, our Legal Department was called upon to take a lead role in overseeing and managing the organization's response. There are a number of reasons why people might turn to legal counsel on these occasions, even though the response involved is not strictly, or even primarily, a legal one. Emotions may rise in high-profile patient cases; staff is appropriately focused on the patient, yet simultaneously concerned that inadvertent actions or responses may jeopardize either themselves or the institution, especially when the police or other government entity is involved. Having an attorney who is knowledgeable about the rules and making sure everyone is following them is reassuring. In particular, the Health Insurance Portability and Accountability Act (HIPAA) is a core concern in any high-profile patient situation as there are both internal and external confidentiality risks, including, but not limited to, curious staff and visitors, attempts from the external media to obtain information, and the understandable desire of staff to correct the record when media reports misinformation or presents a skewed perspective.

Attorneys are also trained to maintain a sense of calm in difficult situations, ask probing questions, and take into consideration every detail of a situation before recommending a course of action, which should generate confidence that the organization's ultimate response is not only legal, but thorough and deliberate. Further, requests from the organization's attorney often carry a certain gravitas. Staff throughout the organization might respond more quickly and comply more precisely when concerned about potential legal ramifications.

For these reasons, attorneys should be ready, willing, and prepared to step up when they find their organizations suddenly immersed in a high-profile patient situation.

The High-Profile Patient with a Low Profile

When the child of a public figure was hospitalized at Connecticut Children's, departments around the hospital sprang into action to ensure that confidentiality and the family's privacy were protected against the extra attention the patient's record could receive from both insiders and outsiders. HIPAA requires covered entities to implement multiple physical, technical, and administrative safeguards to protect the confidentiality and security of any patient's electronic identifiable information. Identifying and implementing these safeguards are likely focused on mitigating risk associated with a breach of information involving the average patient whose information and medical record would not otherwise create extra interest by staff or the public. However, typical safeguards may not suffice in a high-profile patient situation. It is critically important to assess the organization's current safeguards and determine if any additional processes need to be in place to ensure the privacy and security of the high-profile patient.

Identify key stakeholders and their roles

One of the first tasks when dealing with a high-profile patient is to identify all of the key internal stakeholders who need to be involved to ensure that safeguards are overseen with extra diligence during the patient's stay. To limit the number of people who have knowledge of the high-profile patient, it may be important to choose only those stakeholders who have a critical role in overseeing area-specific safeguards. Limiting the number of people who are aware of the situation will also reduce the risk of breaches that might be caused by internal staff.

In determining who should be involved, the attorney for the organization may want to consider creating two groups of stakeholders: (i) those who need to be generally aware in case tangential issues arise (e.g., employee discipline due to unauthorized access to the medical record) and (ii) those who need to be actively involved in the ongoing and routine meetings where updates are provided. The first “general awareness group” should include a representative from each of the departments listed in Table 1 below.

Table 1: General Awareness Group

Billing
The individual responsible for the billing work queues prior to submission to the payers should consider assigning a select number of medical record coders and staff to process the medical claims of the high profile patient. He or she should also determine if it is appropriate to hold the high profile patient’s medical claims in a work queue until the patient is discharged to reduce the number of electronic submissions transmitted to an external entity.
Medical Records
The individual(s) responsible for responding to release of information requests and record restriction requests should monitor and track requests for copies of the high profile patient’s medical record and determine if extra safeguards need to be in place to validate the legitimacy of requests for copies of the patient’s medical record. For example, if the organization typically validates by asking the requestor for patient name and date of birth, Medical Records staff should consider adding one or two extra data points to ensure proper validation.

Table continues

Human Resources

An individual who is responsible for employee relations should ensure that the organization's process for determining the appropriate level of employee discipline addresses patient privacy breaches and that controls are in place to ensure it will be applied consistently. For example, some organizations take the stance that an employee's negligence or willful misconduct should result in automatic termination, while others categorize the event as worthy of disciplinary action, but not necessarily an automatic termination.

Registration

An individual responsible for obtaining pre-authorizations, utilization management, consent forms, etc. should ensure that, if the patient uses an alias, all of the legal documents in the medical record (including admissions and informed consent) use the patient's legal name as opposed to the alias. Registration should work with Nursing to segregate (and keep out of the medical record) the legal forms using the patient's legal name until the patient is discharged. After that, the legal forms should be placed and ultimately maintained in the high-profile patient's medical record.

Information Technology

An individual who is responsible for implementing technical safeguards in the electronic medical record system, registration system, or billing system should address any issues involving the functionality of the additional safeguards implemented for the high-profile patient.

Compliance

The Compliance Officer or someone in the Compliance Department should identify all policies that require employees to keep patient information confidential, to be included in an internal email sent to all employees as a reminder of their respective obligations to protect patient confidentiality—and the potential consequences for not meeting those obligations. This email should be drafted in collaboration with the Corporate Communications employee responsible for transmitting all internal emails.

The second “actively involved group” comprises individuals required at key stakeholder meetings. Table 2 below contains a list of the key stakeholders from departments throughout the organization, and a few of the tasks for which each would be responsible.

Table 2: Key Stakeholders

Nursing Operations	
<i>Who:</i>	This person could be the nursing director responsible for the hospital unit on which the patient is staying.
<i>Role:</i>	<ul style="list-style-type: none"> • Provide medical updates on the patient to the extent necessary so that the group can determine if others need to get involved to ensure the patient’s privacy is continued. • Educate and/or remind his/her staff about the importance of maintaining patient confidentiality and the potential consequences for violating the policy. • Have direct contact and communications with the high-profile family. • Serve as a liaison to the medical staff and other ancillary service providers regarding the patient’s needs while reminding such staff about the importance of keeping the information confidential. • Assign an alias to the patient (and potentially the family members if requested by the family).
Ancillary Clinical Operations	
<i>Who:</i>	The individual or director who is responsible for the rehabilitation and other ancillary services that the patient may be receiving.
<i>Role:</i>	Assign a specific, limited number of staff to care for the high-profile patient, and provide such staff with updates as necessary.

Table continues

Environmental Services

Who: The individual or director who is responsible for the environmental staff.

Role: Assign a specific, limited number of staff to care for the high-profile patient, and provide such staff with updates as necessary.

Information Security

Who: An individual, such as the information security officer, who is responsible for performing routine audits of the electronic medical record.

Role:

- Routinely audit the patient's electronic medical record.
- Determine if any unauthorized individuals accessed the record.
- Investigate any issues that involve inappropriate or unauthorized access to the patient's medical record.
- Implement necessary safeguards in the patient's medical record after he/she is discharged (to address concerns about future requests to obtain copies of the patient's record).

Physical Security

Who: An individual or the director who is responsible for the overall physical security of the organization.

Role:

- To the extent necessary to protect the confidentiality of the patient's family, coordinate different entrances into the facility so that the family can avoid interacting with the general public as much as possible.
- Coordinate the assignment of security officers to accompany the family when entering and exiting the facility.
- Ensure that guests (wanted or unwanted) are appropriately screened upon entering the building.

Table continues

Corporate Communications

Who: An individual who is responsible for public relations.

Role:

- Routinely review the internet and news media to determine if the public has become aware of the high-profile patient's status in the hospital.
- Draft internal communications to all staff that summarize key policies that require everyone to (i) keep patient information confidential and (ii) direct all inquiries from external media to the Corporate Communications Department. Ensure that the message is drafted in a way that does not inform everyone that there is a high-profile patient, but reminds staff about the importance of patient confidentiality (including the potential ramifications for not following such policies).
- Draft external communications and be prepared to respond to both internal and external inquiries.

Legal

Who: An individual, such as the organization's attorney, who is familiar with privacy and security laws.

Role:

- Educate and remind the stakeholders of the intricacies and nuances of the privacy and information security laws as they relate to patient information.
- Serve as the facilitator of the routine update meetings.
- Assess the risk associated with the daily circumstances and make decisions about the change or implementation of the safeguards that are necessary to protect the patient's confidentiality.

Table continues

Concierge

Who: Although it is unlikely that an organization has an employee who serves in this role, a concierge may be assigned to the patient or his/her family to assist with their specific needs and serve as a liaison between the patient/family and the organization. Finding an employee who is personable, understands the importance of delivering great customer service, and would not be intimidated by the high status of the patient (or his/her family) would be an ideal fit. If the organization has a fundraising arm, an individual who works on obtaining major gifts could be a good person to serve as a concierge.

Role:

- Serve as a liaison between the patient (and family) and the organization regarding non-clinical issues.
- Coordinate the non-clinical needs of the patient or family (e.g., security escorts, car services, etc.).

Child and Family Support Services

Who: An individual who can provide, for example, counseling or interpreter services. These services can generally be accessed through this department.

Role: Serve as the social worker and an internal resource for the patient and family, facilitating services that might include interpretation services, relationship management, etc.

Risk Management

Who: Risk manager, preferably with a clinical background, can be invaluable when dealing with the complexities of the patient's care.

Role: Pay attention to the patient's care and identify ways to mitigate potential clinical risks.

While it is atypical to advise several departments of a patient's identity, this proactive approach will help facilitate HIPAA compliance in high-profile patient situations. In addition, identifying the specific role of each stakeholder will set the tone for ensuring that the organization's internal processes are active and effective. The frequency of meetings will dictate how often the individual needs to perform specific tasks.

Frequency of meetings

Due to the high-profile nature of the patient (and his/her family), the circumstances that involve their privacy and confidentiality can drastically change in a moment's notice. It is very important that stakeholders meet on a regular basis where each can provide updates to the entire group on any issues that may have arisen since the last update. When the patient is first admitted, the key stakeholders may consider meeting daily or on a more frequent basis to ensure that everything is in place and that the safeguards are functional and serving their purpose. If things run smoothly and depending on the patient's estimated length of stay, stakeholders can likely transition their update meetings to be less frequent. It may be tempting to discontinue the update meetings if the safeguards are working and there are no privacy incidents; however, we cannot stress enough the importance of ensuring that these meetings continue throughout the patient's *entire* length of stay. The meetings serve as a strong reminder to the stakeholders of the high-profile patient's circumstances and the importance of ensuring that the safeguards remain in place. If all goes well, the update meetings will likely run very quickly. A privacy incident that can ultimately result in a HIPAA-reportable breach is more likely to happen when guards are down, even if only for a brief moment.

The Patient Who Attracts the Media

Additional problems may arise when a patient interacts with the media directly or his/her case attracts media attention. For example,

in the case of *In re Cassandra C.*,¹ the mother of a 17-year-old daughter with Hodgkin's Lymphoma refused, on her daughter's behalf, the recommended medical care. Connecticut Children's remained in the media spotlight from the moment the state's Department of Children and Families (DCF) filed a neglect petition with the Superior Court for Juvenile Matters in October 2014, and long after the Connecticut Supreme Court upheld a lower court ruling granting custody of the minor to DCF over two months later in January 2015. Social media had provided an excellent vehicle for the transmission of information and photos directly from the patient in her hospital room, as well as from her mother, her attorneys, and their supporters.

In another example, an incident on the premises attracted the media spotlight. In February 2005, an 8-month-old baby was found lying on the floor in her hospital room at Connecticut Children's, crying, and critically injured. She had lived at the hospital since birth due to chronic health issues. Upon hearing the baby's distress, a nurse rushed to the baby's room, picked her up and began caring for her. The nurse called a Code Blue and almost immediately, several doctors, nurses, and residents arrived to provide life-saving medical care. One of the nurses who responded to the Code Blue threw a towel over the blood on the floor so that no one would slip on it. Everyone's focus during that moment was on the baby's health. Unfortunately, the baby died six days later while being cared for in the Pediatric Intensive Care Unit (PICU).

Working with the media

In cases like these, the organization must maintain an ongoing dialogue internally to constantly examine the pros and cons of the hospital's participation in the numerous and different forms of social media. In our mature minor case, advocates from throughout the country exploited social media to voice negative opinions and organize protests.

1 All facts pertaining to the Connecticut Children's case are taken from the Connecticut Supreme Court's published written decision on the matter. *In re Cassandra C.*, 316 Conn. 475 (2015).

Silence by the institution's staff members and volunteers can be golden. Of considerable concern in our mature minor case was the potential of a confidentiality breach, not because of trust issues among staff, but because of the inaccuracies being reported in the media. While it may be tempting for staff members and volunteers to want to clarify the inaccuracies and "set the record straight," remaining silent can help avoid any potential HIPAA breaches, maintain patient confidentiality, and keep the conversation one-sided and thus, shorter.

The *organization* should, however, be adept at handling the media and know when to correct inaccuracies as needed. The hospital should designate an individual or team that has received extensive media training to speak on behalf of the organization. While it may seem like an appropriate person to communicate with the media would be the attorney(s) involved in the high-profile patient's case, using an attorney as a spokesperson may be viewed by the media as defensive and therefore not in the best interest of the institution.

Although each case requires its own assessment, the organization should be prepared to keep communication to a minimum, only reacting to media requests when appropriate. Since the organization's staff should stay away from setting the facts straight or defending themselves given HIPAA privacy limitations, the hospital can tell its story through aspirational statements, such as "We act in the best interests of the child, respecting the family"

In Connecticut Children's mature minor case, the doctors providing care to the 17-year-old endured threats and negative publicity while the entire organization received much criticism and an increasing number of threatening calls, emails, and letters. At times, the fear and confusion among staff was palpable. It is important that all of the health care providers and support staff involved in caring for the high-profile patient feel supported, validated, and appreciated for their accomplishments.

Finally, while an organization cannot keep the media from filming outside, any inside shots, such as those sent to the media from the

17-year-old patient's iPad, must not contain information that would violate the privacy rights of any other patient.

At Connecticut Children's, Public Relations and Corporate Communications has spent an enormous amount of time managing the internal and external messages necessitated by situations like these. We have consulted with a crisis management public relations firm that had experience with a similar situation at another children's hospital. We have also reached out to colleagues across the country who generously shared advice and lessons learned and engaged trusted outside counsel to support the involved health care providers with individual concerns.

Preparing for IT threats

During the mature minor case, we were aware of a nearby children's hospital that became the target of hacking by an activist who sought to bring down the hospital's IT system in response to a similar case. Hospital portals and websites were assaulted, followed by a massive influx of malware-laden emails. That children's hospital was generous in sharing information and lessons learned. For example, in response to the threat and the increased assaults on the system (40 times the typical traffic), the hospital activated a coordinated and bold response that included shutting down email, e-prescribing, and external-facing websites. Staff was instructed to communicate through a secure text messaging application. This ordeal showed that having an alternative to email can prove critical to protecting an organization's IT systems. Fortunately, no patient data was compromised at that hospital, no beds were closed, no clinics were cancelled, and the hospital came out with its system intact.

Our email filtering statistics show that currently, only 7.8% of total email volume is "clean," and close to 88% is determined to be some type of threat. It is significant and unfortunate that in one typical month, approximately 300,000 emails out of 3.8 million are legitimate. The Connecticut Children's IT team responds with heightened vigilance and

an action plan, should one need to be activated. Although an increase in activity was noted during the mature minor case, it did not rise to the level of having to close down any of the organization's portals or websites.

Due to the increased vulnerability that can result to an organization's IT system when a high-profile patient is being cared for, investment of resources in IT/cyber security and emergency management should be a major component of such an investment. In addition to investing in IT security and emergency management, the following recommendations should also be considered:

- Take an inventory of the organization's IT system for web applications and email dependence.
- Develop a systems grid that looks at all operations (i.e., development, finance, satellites, research, sub-contractors).
- Review labor and vendor resources.
- Develop a media strategy in case of cyberattack.

Working with public officials

When the care of a patient requires coordination with public officials, it is important to establish common ground and foster mutual respect. Daily communication with the DCF was critical to maintaining control in our mature minor case. DCF Commissioner Joette Katz and DCF Counsel Maureen Duggan worked closely with Connecticut Children's to manage the legal process and maintain open lines of communication so that the organization could avoid public debate of differing opinions.

In the case of the 8-month-old baby, as soon as the patient was taken to the PICU, the floor staff turned their attention to the needs of other patients and families, some of whom were already aware of the situation. Administration, Security, and Risk Management were notified but no one thought to call the police. The baby's fall was viewed as an internal event, potentially a lawsuit, but no one thought of it as a crime. It was

not until several hours later, in the early hours of the next day, that someone notified the police. Connecticut Children's failure to immediately reach out to law enforcement provided us with one of our most important lessons learned. For the next several months, an arduous investigation was conducted, placing caregivers and the institution at risk. In addition to having inadvertently disrupted the crime scene, our delay in calling the police was construed as an attempt to impede the investigation.

As legal counsel for the organization, attorneys should immediately consider whether an event could be construed as one that should be reported to the police. Ensure that any areas, equipment, objects, etc. that could be considered connected to a potential crime scene or relevant to a criminal investigation remain undisturbed to the fullest extent possible. The scene should not be left unattended if the police have not yet arrived. Legal counsel should be present, if possible, to verify the validity of a search warrant and to document the events and follow-up.

Subsequently, we met several times with the representatives from the police department, reviewing all of our policies that were of interest to law enforcement and making changes to several of those policies in response to the suggestions of the police. We also hired a public relations firm to help us manage the message, as well as outside counsel to assist with the law enforcement and regulatory challenges.

Key Policy Points to Consider in High-Profile Cases

Your organization likely has policies on most of the topics listed below, but are they designed to address a high-profile patient scenario? Below are some recommendations for key content to include in your policies to ensure that your organization is ready for a high-profile patient.

Media Relations

- Specify authorized personnel who may respond to media inquiries. Direct all other staff to refer any inquiries to these personnel without comment.
- Staff should not contact the media with a story idea or write opinion pieces (e.g., letters to the editor) in their capacity as hospital employees without prior approval from the Communications Department.
- Staff should avoid using the patient's real name in internal or external communications. Use the alias or the generic term "high-profile patient."
- Generally prohibit external media from taking photographs or granting interviews (on camera, in person, or by phone) with patients, including patients who have been involved in high-profile accidents or news events, during their hospital stay. In certain circumstances this may be permissible if the family wishes to speak to the media, appropriate releases are obtained, and the interview takes place in a way that does not interfere with patient care or the privacy of other patients or staff.

Websites and Social Media

- Prohibit employees from using or disclosing any clinical details or patient identifiable information or posting photos of patients on the internet or any social media forums. This includes making any reference to having treated a VIP or high-profile patient (even if no other information is revealed).
- Restrict use of social media to authorized users who need such access to do their jobs (e.g., Communications staff.)

Name Changes

- Identify a process for assigning an alias to the high-profile patient (and parents, if necessary) in the medical record.
- All legal forms must use the patient's legal name. This may necessitate using paper forms rather than the electronic record.

Confidentiality

- All employees, medical staff, officers, directors, vendors, contractors, volunteers, students, and other agents, regardless of their role/capacity, should sign a confidentiality agreement upon hire.
- Staff should access only the minimum necessary confidential information required to perform their particular functions.
- Staff should immediately notify a supervisor or the Legal/Compliance Department in the event of a suspected or actual breach.
- Employees should be reminded of their obligations under this agreement and the potential consequences of a breach during a high-profile patient scenario.

HIPAA Security Policies

- Identify and implement a mechanism for auditing access to electronic records. Remind staff during high-profile patient situations that access is audited, and unauthorized access is grounds for discipline.
- Implement post-discharge safeguards for high-profile patients (e.g., "break the glass" procedures.)

Law Enforcement Investigations

- In the event of a suspicious occurrence, staff should immediately notify Security to secure the area and contact the police. Do not leave area unattended. Stay until police arrive.
- Without compromising patient care, staff should leave all potential evidence as found.
- Staff should cooperate with law enforcement investigations to the maximum extent possible while being mindful of confidentiality laws with respect to questions about a patient. Staff should contact the Legal Department for guidance on what may be disclosed.
- In the event that law enforcement arrives with a search warrant, staff should notify appropriate departments (e.g., Risk Management and/or Legal) and ask the individual to wait until the representative from that department arrives to verify the validity of the search warrant or court order.
- Law enforcement interviews of patients must be done at a time and in a manner that does not interfere with patient care.

Hospital Emergency Operations Plan

- Plan for activation of an Incident Command Center with appropriate and clear reporting structures.
- Identify a procedure for notification of key departments and individuals of an emerging situation and immediate assessment of the situation. Identify types of events requiring immediate plan activation vs. events to be monitored for possible plan activation. However, do not attempt to catalogue detailed responses for every potential scenario, as many of these types of scenarios are impossible to predict and require some flexibility in the response.

- Define basic staff roles/functions during an emergency. Among others, identify a Public Information Officer who serves as the conduit for information to internal and external stakeholders—including staff, visitors, and families—and the news media, as approved by the Incident Commander. Identify a Security Officer responsible for (i) controlling the flow of media, families, visitors, and others who enter and exit the organization; (ii) overseeing the egress routes to and from the organization; and (iii) overseeing the security and protection of resources and assets.
- Write emergency response plans, keeping in mind that staff will be reading them during an unfamiliar, high-stress situation. Therefore, clarity and ease of use is of paramount importance.
- Include a debriefing process to identify and implement lessons learned from an incident.

Conclusion

Like most health care institutions, Connecticut Children's has had its share of high-profile patients and the challenges that accompany that distinction. We find ourselves facing these challenges at the intersection of increased privacy requirements and an explosive proliferation of access to information. Our experiences have taught us to be proactive, anticipating as many potential obstacles as possible, as early as possible; working with parents to get them on board with recommendations that would be in the best interest of the patient; meeting with police before they are actually needed so that trust between law enforcement and the hospital can be nurtured and strengthened; and being prepared to act boldly when the situation warrants it, such as in the case of the children's hospital that shut down email when its IT system was being attacked.

On the other hand, the true facts of a case can be lost in all of the emotions that naturally arise when a high-profile patient scenario presents itself, or when a tragic incident creates the high profile situation. The reporting of such patients or events can become media-driven, leading to inaccuracies and increasing threats and vulnerabilities to the hospital's workers and operational systems. Rely on colleagues, both internal and external, who have experienced a similar ordeal. Caring for a high-profile patient or handling a high-profile incident usually requires a team. Without any one player, the team suffers and a successful outcome for the patient and the institution may be placed in jeopardy.

The hospital legal department at Connecticut Children's is small but involved in many areas of the hospital's operations, which is not uncommon. Hospital legal departments exist so that everyone who is directly and indirectly involved in the continuum of patient care—from the physician to the risk manager to housecleaning staff—can focus on caring for the patient and providing the patient with the best type of environment that will expedite his or her recovery.