*Anita Hakala-Homework due****Sunday, November 20 at 11:55 PM****(Required)*

1. Check Your Understanding

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **9.1** | **9.2** | **9.3** | **9.4** |
| **1.** | B | A | B | B |
| **2.** | C | C | A | A |
| **3.** | B | D | C | D |
| **4.** | B | B | B | C |
| **5.** | B | D | D | B |
| **6.** | C | A | C | A |
| **7.** | B | B | A | A |
| **8.** | C | B | D | A |
| **9.** | C | B | C | D |
| **10.** | C | A | D | C |

2 Define:

**Access report:** Report that provides a list of individuals who accessed patient information during a given period

**Administrative simplification:** As amended by HITECH, authorizes HHS to 1.) adopt standards for transactions and code sets that are used to exchange health data; 2.) adopt standard identifiers for health plans, health care providers, employers, and individuals for use on standard transactions; and 3.) adopt standards to protect the security and privacy of personally identifiable health information (45 CFR Parts 160, 162, and 164 2013)

**ARRA:** The purposes of this act include the following: 1.)to preserve and create jobs and promote economic recovery; 2.) to assist those most impacted by the recession; 3.) to provide investments needed to increase economic efficiency by spurring technological advances in science and health; 4.) to invest in transportation, environmental protection, and other infrastructure that will provide long-term economic benefits; 5.) to stabilize state and local government budgets, in order to minimize and avoid reductions in essential services and counterproductive state and local tax increases.

**Admissibility:** The condition of being admitted into evidence in a court of law.

**Breach:** Under HITECH, the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part that compromises the security or privacy of the protected health information (45 CFR 164.402 2013)

**BA:** Business associate- 1.) A person or organization other than a member of a covered entity’s workforce that performs functions or activities on behalf of or affecting a covered entity that involve the use of individually identifiable health information; 2.) As amended by HITECH, with respect to a covered entity, a person who creates, receives, maintains, or transmits PHI for a function or activity regulated by HIPAA, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities, billing, benefit management, practice management, and repricing or provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services (45 CFR 160.103 2013)

**CLIA:** Clinical Laboratory Improvement Amendments od 1988, established quality standards for all laboratory testing to ensure the accuracy, reliability, and timeliness of patient test results regardless of where the test is (Public Law 90-174 1967)

**Confidentiality:** 1.) a legal and ethical concept that establishes the healthcare provider’s responsibility for protecting health records and other personal and private information from unauthorized use of disclosure; 2.) As amended by HITECH, the practice that data or information is not made available or disclosed to unauthorized persons or processes (45 CFR 164.304 2013)

**Complaint:** In litigation, a written legal statement from a plaintiff that initiates a civil lawsuit

**Consent:** 1.) a patient’s acknowledgement that he or she understands a proposed intervention, including that intervention’s risks, benefits, and alternatives; 2.) The document signed by the patient that indicates agreement that protected health information can be disclosed

**Covered entity:** (CE) As amended by HITECH, 1.) a health plan, 2.) a healthcare clearinghouse, 3.) a healthcare prover who transmits any health information in electronic form in connection with a transaction covered by this subchapter (45 CFR 160.103 2013)

**Deidentified information:** Information where personal characteristics have been stripped from it in such a way that it cannot be later constituted or combined to reidentify an individual; it is commonly used in research

**HHS:** Department of Health and Human Services- The cabinet-level federal agency, and principal agency for protecting the health of all Americans and providing essential human services, especially for those who are at least able to help themselves

**DRS:** A Designated Record Set: as amended by HITECH: 1. A group of records maintained by or for a covered entity that is: (i) The medical records and billing records about individuals maintained or for a covered health provider, (ii) The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or (iii) Used, in whole or in part, by or for the covered entity to make decisions for individuals 2. For purposes of this paragraph, the term means any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for a covered entity (45CFR 164.501 2013)

**E-discovery**: refers to Amendments to Federal Rules of Civil Procedure and Uniform Rules Relating to Discovery of Electronically Stored Information; wherein audit trails, the source code of the program, metadata, and any other electronic information that is not typically considered the legal health record is subject to motion for compulsory discovery

**Facility directory:** A directory of patients being treated in a healthcare facility

**FRCP:** Federal Rules of Civil Procedure-Rules established by the US Supreme Court setting the “rules of the road” and procedures for federal court cases. FRCP include electronic records an continue to be very important as benchmarks in how these records can be used in courts, not only in federal, but state and other courts as well (Public Law 97-462 1983)

**FRE:** Federal Rules of Evidence- Rules established by the US Supreme Court guiding the introduction and use of evidence in federal court proceedings that are an important benchmark for state and other courts. FRE governs what and how electronic records may be used, and the roles of record custodianship.

**FTC:** Federal Trade Commission- An independent federal agency tasked with dealing with two areas of economics in the United States: consumer protection and issues having to do with competition in business

**HITECH:** Health Information Technology for Economic and Clinical Health Act- Legislation created to promote the adoption and meaningful use of health information technology in the United States. Subtitle D of the act provides for additional privacy and security requirements that will develop and support electronic health information, facilitate information exchange, and strengthen monetary penalties. Signed into law on February 17, 2009, as part of ARRA (Public Law 111.5 2009)

**HIPAA:** Health Insurance Portability and Accountability Act- The federal legislation enacted to provide continuity of health coverage, control fraud and abuse in healthcare, reduce healthcare costs, and guarantee the security and privacy of health information; limits exclusion for pre-existing medical conditions, prohibits discrimination against employees and dependents based on health status, guarantees availability of health insurance to small employers, and guarantees renewability of insurance to all employees regardless of size; requires covered entities(most healthcare providers and organizations) to transmit healthcare claims in a specific format and to develop, implement, and comply with the standards of the Privacy Rule and the Security Rule; and mandates that covered entities apply for and utilize national identifiers in HIPAA transactions (Public Law 104-191 1996)

**Hearsay:** A written or oral statement made outside of court that is offered as court evidence

**Legal hold:** A communication issued because of current or anticipated litigation, audit, government investigation, or other such matters that suspend the normal disposition or processing of records. Legal holds can encompass business procedures affecting active data, including, but not limited to, back-up tape recycling. The specific communication to business or IT organizations may also be called a “hold”, “preservation order”, “suspension order”, “freeze notice”, “hold order”, or “hold notice”

**Medical identity theft:** A type of healthcare fraud that includes both financial fraud and identity theft, it involves either (a) the inappropriate or unauthorized misrepresentation of one’s identity (for example, the use of one’s name and Social Security number) to obtain medical services or goods, or (b) the falsifying of claims for medical services in attempt to obtain money.

**Minimum necessary:** A standard that require that uses, disclosures, and requests must be limited to only the amount needed to accomplish an intended purpose

**ONC:** Office of the National Coordinator for health Information Technology which is the principle federal entity charged with coordination of nationwide efforts to implement and use the most advanced health information technology and electronic exchange of health information. The position of National Coordinator was created in 2004, through an executive order, and legislatively mandated in the HITECH Act of 2009

**Personal representative:** Person with legal authority to act on a patient’s behalf

**Preemption:** In law, the principle that a statute at one level supersedes or is applied over the same or similar statute at a lower level (for example, the federal HIPAA privacy provisions trump the same or similar state law except when the state is more stringent)

**PHI:** Protected Health Information- As amended by HITECH, individually identifiable health information: (1.) except as provided in paragraph (2) of this definition, that is ☹i) transmitted by electronic media; (ii) maintained in electronic media; or (iii) transmitted or maintained in any other form or medium. (2) Protected health information excludes individually identifiable health information in (i) education records covered by the Family Educational Rights and Privacy Act, as amended, 20 USC 1232g; (ii) in records described in 20 USC 1232g (a) (4)(B) (iv); (iii) in employment records held by covered entity in its role as an employer; and (iv) regarding a person who has been deceased for more than 50 years (45 CFR 160.103 2013)

**Red Flags Rule:** Consists of five categories of red flags that are used as triggers to alert the organization to a potential identity theft; the categories are 1.) alerts, notifications, or warnings from a consumer reporting agency; 2.) suspicious documents; 3.) suspicious personally identifying information such a a suspicious address; 4.) unusual use of, or suspicious activity relating to a covered account; 5.) Notices from customers, victims of identity theft, law enforcement authorities, or other businesses about possible identity theft in connection with an account

**Right to request amendment:** One may request that a covered entity amend PHI or a record about the individual in a designated record set

**Spoliation:** The act of destroying, changing, or hiding evidence intentionally

**TPO:** Treatment, payment and operations- The privacy rule provides for a number of exceptions for PHI that is being used or disclosed for TPO purposes; treatment means providing, coordinating, or managing healthcare or health-related services by one or more healthcare providers; payment includes activities by a health plan to obtain premiums, billing by healthcare providers or health plans to obtain reimbursement, claims management, claims collection, review of medical necessity of care, and utilization review; the Privacy Rule provides a broad list of activities that are healthcare operations that includes quality assessment and improvement, case management, review of healthcare professionals’ qualifications, insurance contracting, legal and auditing functions, and general business management functions such as providing customer service and conducting due diligence

**Warrant:** A judge’s order that authorizes law enforcement to seize evidence and conduct a search

**Sale of information:** Addressed specifically by ARRA, which prohibits a covered entity or Business Associate (BA) from selling (receiving direct or indirect compensation) in exchange for an individual’s PHI without that individuals authorization; the authorization must also state whether the individual permits the recipient of the PHI to further exchange the PHI for compensation

3. You should always have the actual language of the HIPAA privacy regulation at your fingertips should questions about i**nterpretations** arise.

  1. Review Breach Notification. Evaluate the information offered and how to report a breach.

OCRPrivacy@hhs.gov. The breach must be reported electronically ([Submit a Notice for a Breach Affecting 500 or More Individuals](https://ocrportal.hhs.gov/ocr/breach/breach_form.jsf)) ([Submit a Notice for a Breach Affecting Fewer than 500 Individuals](https://ocrportal.hhs.gov/ocr/breach/breach_form.jsf)) in 60 calendar days from the discovery of the breach if it affect >500 people. If it is < 500 people it must be reported by 60 calendar days by the end of the calendar year the breach occurred. The whole process can be found in the federal Register [45 C.F.R. § 164.408](https://www.gpo.gov/fdsys/granule/CFR-2011-title45-vol1/CFR-2011-title45-vol1-sec164-408). The length of time an organization has to report the information seem to be long, allowing for that information to travel anywhere and to anybody. As an individual, I would want to have that information much sooner than that if my information was part of that breach.

   2. Review Special Topic and choose Health Information Technology.   Visit the various sites and summarize your findings as they relate to this chapter.

 <http://www.hhs.gov/hipaa/for-professionals/index.html>

This website offers area on privacy, security, breach notification. Compliance and enforcement, special topics, patient safety, covered entities and business, training and resources, FAQs for professionals and other administrative and simplification rules directed to professionals. It is a much more explicit area to find all the information a professional may need to understand HIPAA and how it relates to the individual professional. The book seems to highlight many of the areas, but this site is an excellent resource to answer and educate professionals on their role, rules and laws and how to understand any items in HIPAA that may seem confusing.

4. Visit the State of Maine website.

 What are the various state laws related to ownership of the health record?

| **Statute/Regulation** | **Description** |
| --- | --- |
| [Access - 10-144-110 Me. Code R. § 19.J](http://www.healthinfolaw.org/state-law/access-10-144-110-me-code-r-%C2%A7-19j) | Skilled Nursing Facilities must allow each patient and/or representative to inspect his or her records within 24 hours of a request.  The... |
| [Access to recorded personal information - Me. Rev. Stat. tit. 24-A, § 2210](http://www.healthinfolaw.org/state-law/access-recorded-personal-information-me-rev-stat-tit-24-%C2%A7-2210) | If any consumer, after proper identification, submits a written request to an insurer for access to recorded personal information about the consumer... |
| [Assessments, Service Plans and Consumer Records - 10-144-117 Me. Code R. § 8](http://www.healthinfolaw.org/state-law/assessments-service-plans-and-consumer-records-10-144-117-me-code-r-%C2%A7-8) | Every person attending an adult day service program must have a comprehensive written assessment.  It must be given starting no later than the... |
| [Authentication of Hospital Medical Records - 10-144-112 Me. Code R. § XII.F](http://www.healthinfolaw.org/state-law/authentication-hospital-medical-records-10-144-112-me-code-r-%C2%A7-xiif) | All entries into a patient’s medical record must either be signed or electronically authenticated by the treating physician or practitioner.... |
| [Clinical Records - 10-144-110 Me. Code R. § 19.A](http://www.healthinfolaw.org/state-law/clinical-records-10-144-110-me-code-r-%C2%A7-19a) | Skilled Nursing Facilities must maintain clinical records on every resident.  The records must include all current clinical information... |
| [Consumer information - Me. Rev. Stat. tit. 22, § 1718](http://www.healthinfolaw.org/state-law/consumer-information-me-rev-stat-tit-22-%C2%A7-1718) | Every hospital or ambulatory surgical center must, upon request by an individual, provide the average charge for any inpatient service or outpatient... |
| [Consumer Records - 10-144-113 Me. Code R. § 10](http://www.healthinfolaw.org/state-law/consumer-records-10-144-113-me-code-r-%C2%A7-10) | For each individual that receives assisted living services, the program must keep a record that includes identifying information of the consumer and... |
| [Content of Hospital Medical Records - 10-144-112 Me. Code R. § XII.E](http://www.healthinfolaw.org/state-law/content-hospital-medical-records-10-144-112-me-code-r-%C2%A7-xiie) | All information contained in a patient’s hospital medical record must be authenticated, pertinent and timely.  There must be enough... |
| [Filing and Retrieval of Hospital Patient Medical Records - 10-144-112 Me. Code R. § XII.D.](http://www.healthinfolaw.org/state-law/filing-and-retrieval-hospital-patient-medical-records-10-144-112-me-code-r-%C2%A7-xiid) | All patient medical records must be readily available and filed in a manner that allows for prompt retrieval.  The record department must be... |
| [Health Care Services - 10-144-118 Me. Code R. § 10](http://www.healthinfolaw.org/state-law/health-care-services-10-144-118-me-code-r-%C2%A7-10) | Prior to a patient’s admission, a physician must gather the patient’s medical history, current medical findings and certify that the... |
| [Inactive Clinical Records - 10-144-110 Me. Code R. § 19.D](http://www.healthinfolaw.org/state-law/inactive-clinical-records-10-144-110-me-code-r-%C2%A7-19d) | All inactive clinical records must be retained for the time required by State law or 5 years from the date of the patient’s discharge,... |
| [Itemized bill - 10-144-112 Me. Code R. § 3.5.7](http://www.healthinfolaw.org/state-law/itemized-bill-10-144-112-me-code-r-%C2%A7-357) | All hospitals must give written notice to all patients that they have the opportunity to request, upon discharge, to obtain a copy of an itemized... |
| [Itemized bills - Me. Rev. Stat. tit. 22, § 1712](http://www.healthinfolaw.org/state-law/itemized-bills-me-rev-stat-tit-22-%C2%A7-1712) | Patients have the right, at the time of discharge, to receive an itemized bill upon request.  The request may be made by the patient or patient... |
| [Medical Records - 10-144-125 Me. Code R. § 4.I](http://www.healthinfolaw.org/state-law/medical-records-10-144-125-me-code-r-%C2%A7-4i) | Ambulatory Surgical Facilities must keep complete, comprehensive and accurate medical records to ensure proper patient care.  Each patient must... |
| [Miscellaneous Records - 10-144-110 Me. Code R. § 19.C](http://www.healthinfolaw.org/state-law/miscellaneous-records-10-144-110-me-code-r-%C2%A7-19c) | Miscellaneous records shall be maintained and retained as follows: |
| [Patient access to hospital medical records - Me. Rev. Stat. tit. 22, § 1711](http://www.healthinfolaw.org/state-law/patient-access-hospital-medical-records-me-rev-stat-tit-22-%C2%A7-1711) | All patients are allowed a copy of their medical record after being discharged from a state-licensed hospital.  In order to obtain copies of his... |
| [Patient access to treatment records; health care practitioners - Me. Rev. Stat. tit. 22, § 1711-B](http://www.healthinfolaw.org/state-law/patient-access-treatment-records-health-care-practitioners-me-rev-stat-tit-22-%C2%A7-1711-b) | All patients are allowed a copy of their medical records that are on file with their health care practitioner.  In order to obtain a copy of his... |
| [Patient Record Retention for Hospitals - 10-144-112 Me. Code R. § XII.B](http://www.healthinfolaw.org/state-law/patient-record-retention-hospitals-10-144-112-me-code-r-%C2%A7-xiib) | All patient records must be kept for a period of 7 years.  If the patient is a minor, the records must be retained for at least 6 years after... |
| [Patient/Client Records - 10-144-119 Me. Code R. § 7.F](http://www.healthinfolaw.org/state-law/patientclient-records-10-144-119-me-code-r-%C2%A7-7f) | Each patient utilizing a home health care service must have an identifiable clinical record that is maintained by the service provider.  The... |
| [Record retention - 10-144 ME. CODE R. Ch. 112 § 3.5.5](http://www.healthinfolaw.org/state-law/record-retention-10-144-me-code-r-ch-112-%C2%A7-355) | Hospitals must retain patient records for 7 years. In the case of minor patients, records must be retained for 6 years past the minor’s 18th... |
| [Records - 10-144-120 Me. Code R. § 5.I](http://www.healthinfolaw.org/state-law/records-10-144-120-me-code-r-%C2%A7-5i) | Hospice programs must maintain records of, at a minimum, care plans of interdisciplinary teams, progress notes regarding the families receiving... |
| [Records - 10-144-126 Me. Code R. § 5.G](http://www.healthinfolaw.org/state-law/records-10-144-126-me-code-r-%C2%A7-5g) | An End Stage Renal Disease facility must keep, at a minimum, individual patient care clinical records, personnel files for all staff, records of... |
| [Records Retention - 10-144-126 Me. Code R. § 5.H](http://www.healthinfolaw.org/state-law/records-retention-10-144-126-me-code-r-%C2%A7-5h) | Records should be retained for at least 7 years post date of discharge, unless stated differently by the state.   |
| [Retention of Records - 10-144-110 Me. Code R. § 19.B](http://www.healthinfolaw.org/state-law/retention-records-10-144-110-me-code-r-%C2%A7-19b) | The following current records shall be available and retained at the nurses station as indicated. |
| [Retention of Records - 10-144-126 Me. Code R. § 5.J](http://www.healthinfolaw.org/state-law/retention-records-10-144-126-me-code-r-%C2%A7-5j) | All clinical and business records must be kept by the program for 5 years from the date of patient discharge. |
| [Retention of Records - 10-144-126 Me. Code R. § 5.J](http://www.healthinfolaw.org/state-law/retention-records-10-144-126-me-code-r-%C2%A7-5j-0) | All clinical and business records must be kept by the program for 5 years from the date of patient discharge. |
| [Transfers and Discharges - 10-144-110 Me. Code R. § 19.F](http://www.healthinfolaw.org/state-law/transfers-and-discharges-10-144-110-me-code-r-%C2%A7-19f) | When a resident is transferring within a Skilled Nursing Facilities, the current resident record may be continued.  However, before a facility... |

5. Evaluate/summarize the following website and information that is offered.

<http://www.hhs.gov/ocr/index.html>

 Through the federal civil rights laws and Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, the Office for Civil Rights (OCR) protects fundamental nondiscrimination and health information privacy rights by:

* Teaching health and social service workers about civil rights, health information privacy, and patient safety confidentiality laws
* Educating communities about civil rights and health information privacy rights
* Investigating civil rights, health information privacy, and patient safety confidentiality complaints to identify discrimination or violation of the law and take action to correct problems.

The site also offers information on how to file a Health Information privacy or security complaint, that can be filed by anyone via mail, fax or via the [OCR Complaint Portal](https://ocrportal.hhs.gov/). It is also available in several languages. It provides information on discrimination, a special section for providers, and many other educational and informational areas.

6.Retrieve 2 articles from the internet that have been written in the past year on privacy compliance. Summarize the important concepts. What have you discovered from this search that is not addressed in this chapter?

***“A Perspective on “Who’s Minding the Store?” in Healthcare”***

This article discusses the state of electronic Health Information and the magnitude of breaches in the healthcare sector with over 113 million breaches if individual health records in 2015 alone. The GAO is calling for healthcare organizations to align with the NIST Cybersecurity Framework. The problem seems to be that there are guidelines to meet the HIPAA demands, but not much guidance on the how-to necessary. The “safeguarding of information must be carefully balanced against the need for access to mission critical patient information”. It also discusses the vast information regarding HIPAA, but not necessarily how to comply, leaving the healthcare industry in limbo. The article closes with, “Guidance serves its purpose by helping to lead the way or provide helpful pointers—but it cannot “do” the necessary work to ensure compliance or robust security for healthcare organizations.  We, as a healthcare sector must do better by being more proactive about cybersecurity.  After all, patient lives (and their data) are very much on the line”.

What I learned from this article is the overwhelming number of health record breaches, not specific in the book and the report that implies how must further the industry must go to decrease these numbers. I didn’t realize just how insecure our health care system can be.

**Gone phishin': Mayo Clinic shares tips for fending off attacks**

“Security professionals should begin by making anti-malware efforts relevant and routine. From there, leverage the technology you have and make sure users know that software can only do so much to protect them”.  Mark Parkulo, MD, of the Mayo Clinic said that employees sometimes have a tendency to think the organization would not let malicious email through and that can lead to problems.

By [Bill Siwicki](http://www.healthcareitnews.com/content/bill-siwicki)

October 05, 2016

The Mayo clinic actually sends “phishing” emails to their staff to try to get them to click on them. They do this as a way to continue education and keep employees from accidently clicking on an email that can create a cyberattack. They have found that by “phishing” their employees will get good at responding appropriately to those types of email, but without continuation of the effort, employees get “lax” and start making mistakes.

“When it comes to protecting against nefarious phishers overall, Frain said there are three overarching principles: technology, process and people.

“It’s important that you leverage the technology you have and recognize and use it to its fullest capacity,” she said. “There are lots of decisions that can be made in setting up filtering in what you let in or out. In healthcare, that gets much more complex because we are accustomed to working with all sorts of individuals and businesses that other industries do not have to deal with.”

The second principle is understanding business processes. Healthcare organizations must bring transparency to the different groups within the organization and the processes these groups use to exchange information, Frain said.

“We spend a lot of time with our patient care providers and supply chain folks, for example, talking them through what are pitfalls we can fall into when we go outside of our normal business processes,” she explained. “So, for example, providers, push patient communication to the patient portal to exchange that kind of information. And supply chain folks, go to the defined processes and avoid one-off exceptions.”

The second component segues into the third, which is people.

“There is no level of technology that can protect an organization from every motivated attacker,” Frain said. “We have to raise the collective awareness of employees so they take a momentary pause as they go through their e-mails.”

From this article, I learned the importance of employee education when it comes to cybercrime. It is very important that healthcare organizations are relentless when dealing with “technology, process and people” to try to prevent the theft of PHI.

7. Do you think there are problems with any of the HIPAA Privacy rule's exceptions to the authorization requirement?

Do the exceptions minimize patient privacy? In way they do, but many of them seem necessary.

Are there too many exceptions?

Are there other exceptions that you would include if you were asked to become involved in revising the law?

***Law Enforcement Purposes -*** *Protected health information may be shared with law enforcement officials under the following circumstances:* ***1.*** *As required by law to adjudicate warrants or subpoenas.* ***2.*** *To locate a suspect, witness, or fugitive.* ***3.*** *Provide law enforcement officials with information on the victim, or suspected victim, of a crime.* ***4****. To notify law enforcement in the case of a suspicious death, which may have resulted from criminal activity.* ***5****. As evidence of a crime that occurred in the facility of a covered entity.* ***6****. A covered entity may provide PHI in the case of an emergency involving one of its patients, even if the incident occurred offsite. Also, to inform law enforcement about a possible crime, victims, perpetrators, or location thereof.*

*-* ***Serious Threat to Health and Safety****- PHI can be released without consent to law enforcement officials to aid in the capture of an escaped prisoner or a violent criminal. Protected health information can also be released if there is credible reason to believe that there is an imminent threat to an individual or the public at large.*

The Area I have the most concern about are the cases which involve law enforcement. It seems that the interpretation by hospital personnel vs police officers are a little different. As a nurse, I am always most concerned about the care provided to the individual to meet their healthcare needs. In some cases I have had police officers walk into an emergency department room, during treatment, and agitate the patient more than they are agitated already, which then affects patient care. There is a time and place for everything and I think we need to be respectful of each other and our roles and settings. I truly understand the need and the importance of this exception, but some of the hospitals I have worked in have actually written policies about when and where police officers can go.

I don’t think there are too many exceptions.

I would need more experience and research as to whether or not I would add more exceptions.