Technology Tightrope: Balancing Digital Advances With Patient Safety and Risk Concerns

Today's Moderator

Today's moderator is Joyce Bruce, RN, MSN, JD, CPHRM, AVP, MedPro Group (Joyce.Bruce@medpro.com)

Joyce provides comprehensive services to healthcare systems, hospitals, and clinics in the Midwest. She has more than 20 years of experience in the healthcare industry working in clinical practice, hospital administration, law, and consulting.

Joyce's extensive clinical leadership includes experience as director of nursing in tertiary and pediatric facilities. In these roles, she led the development of quality programs, delivery of care models, and clinical care paths, including creation of data collection systems. In addition to her healthcare background and expertise, Joyce's legal experience includes insurance defense, criminal defense, and healthcare law.

Joyce is a graduate of Indiana University with a bachelor of science degree in nursing and a master of science degree in nursing administration. Joyce earned her juris doctorate from Indiana University–Indianapolis. She is a member of the Indiana Bar, Ohio Bar, American Society for Healthcare Risk Management, the American Association of Nurse Attorneys, and Ohio Society for Healthcare Risk Management. She is also a certified professional in healthcare risk management.

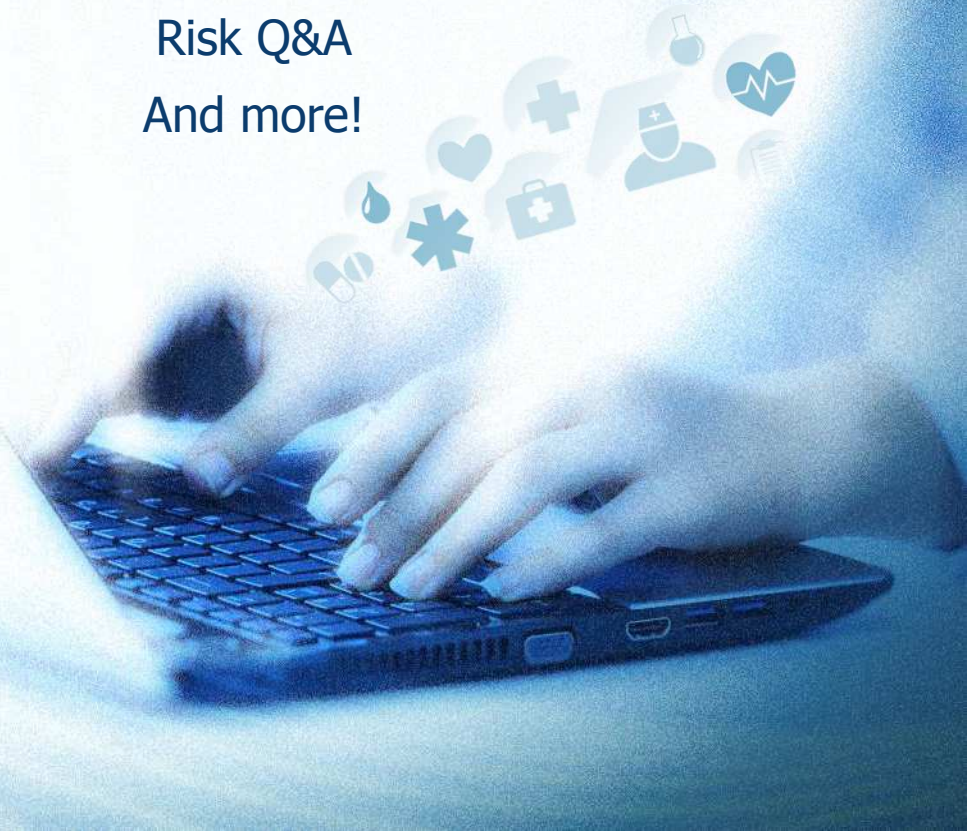
Are you aware of our vast resources?

Join Us on Twitter

Join us on Twitter @MedProProtector!

Risk management and patient safety information delivered in a convenient, flexible format

- Articles
- Announcements
- Resources
- Videos
- Tools
- Case studies
- Risk Q&A
- And more!



Not on Twitter? Give It a Try!

Twitter is an easy, quick way to stay current with healthcare news and trends, receive information and resources, connect with individuals and organizations, and receive risk management info from MedPro! Opening an account is simple — visit www.twitter.com.

Designation of continuing education credit

Medical Protective is accredited by the Accreditation Council for Continuing Medical Education (ACCME) to provide continuing medical education for physicians.

Medical Protective designates this live activity for a maximum of 1.0 AMA PRA Category 1 Credits™. Physicians should claim only the credit commensurate with the extent of their participation in the activity.

Academy of General Dentistry™
PACE
Program Approval for Continuing Education

The Medical Protective Company is designated as an Approved PACE Program Provider by the Academy of General Dentistry. The formal continuing dental education programs of this program provider are accepted by AGD for Fellowship/Mastership and membership maintenance credit. Approval does not imply acceptance by a state or provincial board of dentistry or AGD endorsement. The current term of approval extends from October 1, 2011, to September 30, 2015. Provider ID 218784.

The Medical Protective Company designates this continuing education activity as meeting the criteria for up to 1 hour of continuing education credit. Doctors should claim only those hours actually spent in the activity.

Disclosure

Medical Protective receives no commercial support from pharmaceutical companies, biomedical device manufacturers, or any commercial interest.

It is the policy of Medical Protective to require that all parties in a position to influence the content of this activity disclose the existence of any relevant financial relationship with any commercial interest.

When there are relevant financial relationships, the individual(s) will be listed by name, along with the name of the commercial interest with which the person has a relationship and the nature of the relationship.

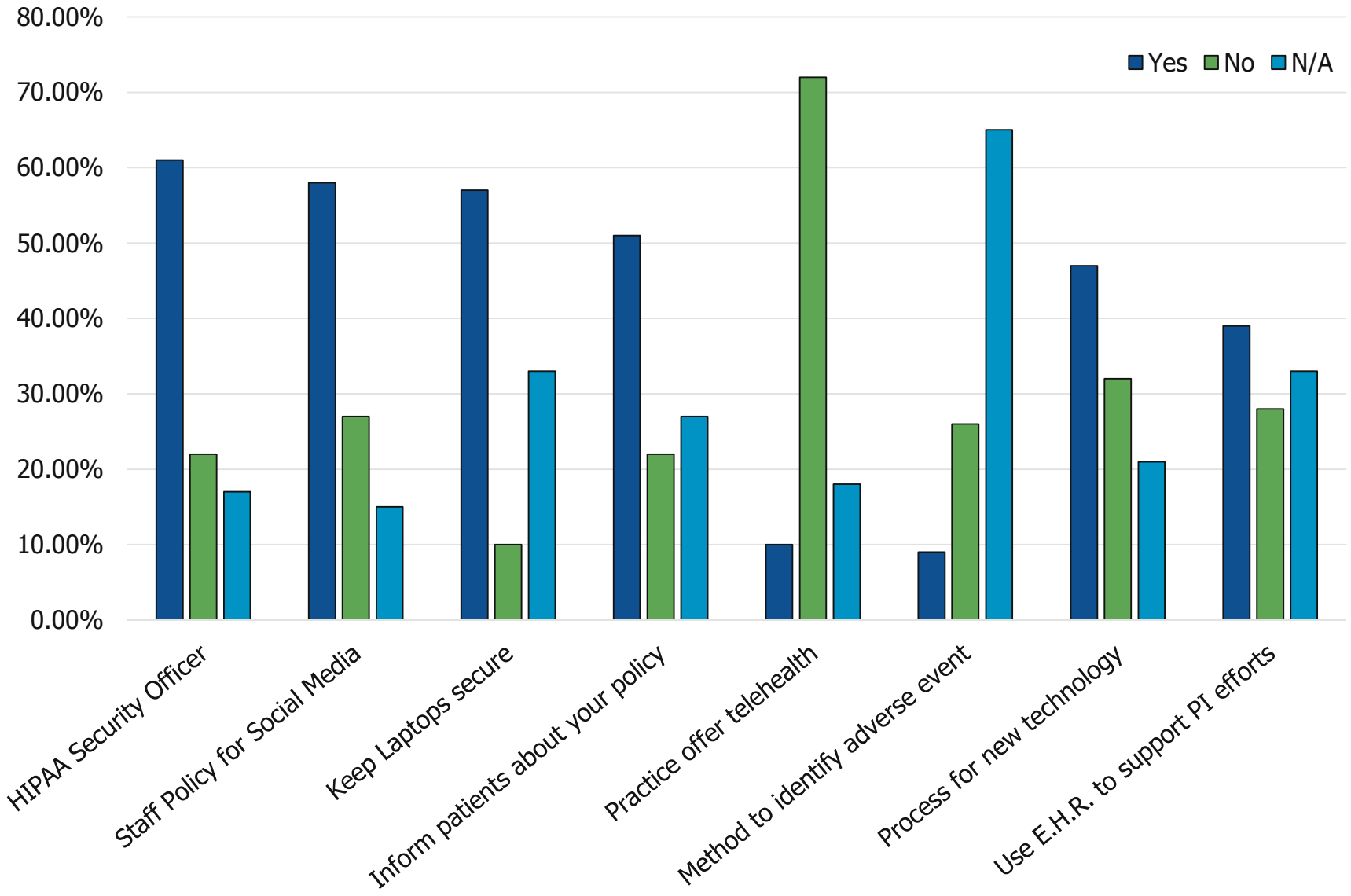
Today's faculty, as well as CE planners, content developers, reviewers, editors, and Patient Safety & Risk Solutions staff at Medical Protective have reported that they have no relevant financial relationships with any commercial interests.

Objectives

At the conclusion of this program, you should be able to:

- Explain why selection, training, and competency are top risk concerns for all new technologies.
- Understand risks associated with social media/ electronic communication and identify key areas for consideration in the development of social media policies.
- Cite barriers and risks associated with telehealth, and describe several strategies that can help address telehealth liability concerns.

Registration Polling Results



Today's program

Today's speaker is Rachel Rosen, RN, MSN, AVP, Medical Protective (Rachel.Rosen@medpro.com)

Rachel has more than 20 years of experience in patient safety, quality, and risk management — both as an internal leader and as an external consultant.

Her healthcare industry customers have included multi-hospital systems, large acute hospitals, long-term acute care facilities, critical access hospitals, healthcare services, and managed care organizations.

Rachel has extensive experience in standards preparation and compliance, strategic organizational improvement planning and implementation, quality measurement, patient satisfaction, and medical staff quality and peer review.

Rachel is a graduate of Ball State University with a bachelor of science degree in nursing, and she earned a master of science degree in nursing administration from Indiana University. Rachel is a member of the American Society for Healthcare Risk Management and the Indiana Society for Healthcare Risk Management.

Today's program

Today's speaker is Beth Michel, MLD, CPHRM, Clinical Risk Management Consultant, Medical Protective (Beth.Michel@medpro.com)

Beth has more than 15 years of experience in medical malpractice litigation defense, data analysis, patient safety, quality improvement, and risk management. She has served both as a paralegal in the insurance industry and as an internal leader in hospitals.

Beth is experienced in directing root cause investigations of serious safety events, and has led performance improvement efforts to implement and measure the effect of change on healthcare outcomes.

Beth is a graduate of Saint Mary-of-the-Woods College with a bachelor of arts degree in paralegal studies and a master of leadership development degree. She is a member of the American Society for Healthcare Risk Management and the Indiana Society for Healthcare Risk Management. Beth is also a certified professional in healthcare risk management.

Specific areas for review

Data security

Electronic communication

Electronic health records

Telemedicine

New technologies

Why talk about data security?

- Stolen health information is more valuable than stolen social security numbers.
- Increasing numbers of healthcare providers are reporting privacy breaches.
- Growing automation and adoption of EHRs exacerbates the risk of privacy breaches.

"An Evolving Risk." Healthcare Risk Management Review, Annual 2014/15

Case study: Postsurgical pictures on Instagram

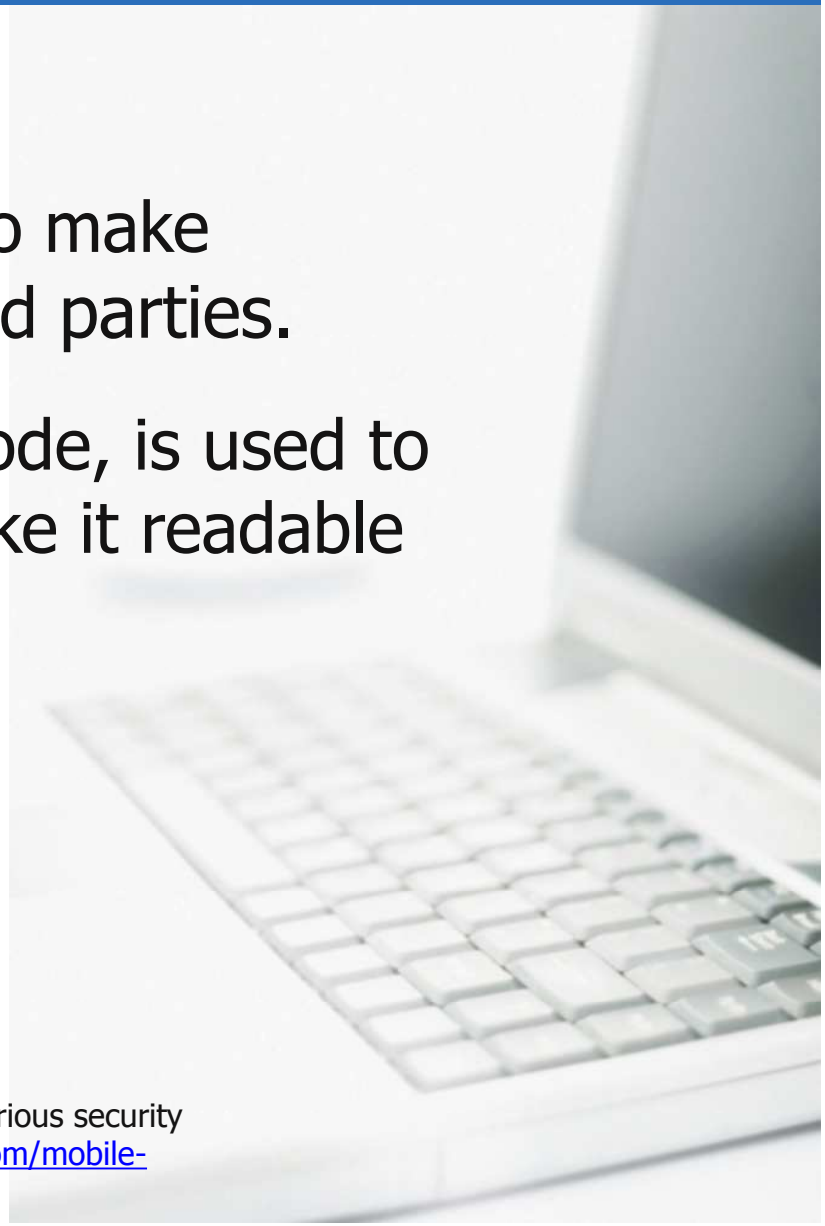
Scenario	Successful bite adjustment and cosmetic veneer procedures performed by dentist; patient consented via Facebook message to physician office posting "after" pictures on Instagram.
Case Overview	Within 2 hours of photo being placed on Instagram, claimant contacted physician office and asked that it be removed.
Outcome	Claim filed, even though photo was immediately removed; alleged violation of rights, negligence, breach of fiduciary duty, breach of contract, and infliction of emotional distress.
Key Issue	Consent did not include all required HIPAA elements.

Privacy and security risks

- Email and texting — Is it encrypted and secure?
- General internet use
- Social media posts
- Staff-owned electronic devices (laptops, tablets, smartphones)
- Flash drives/disks
- Charts/media taken out of office/facility
- Failure of back-up devices

The importance of encryption

- Encryption is a method used to make information unreadable by third parties.
- A key, like a decoder ring or code, is used to decrypt the information to make it readable again.



Rashid, F. Y. (2013, December 7). Majority of mobile apps have serious security flaws. PC Magazine. Retrieved from http://securitywatch.pcmag.com/mobile-apps/318686-majority-of-mobile-apps-have-serious-security-flaws

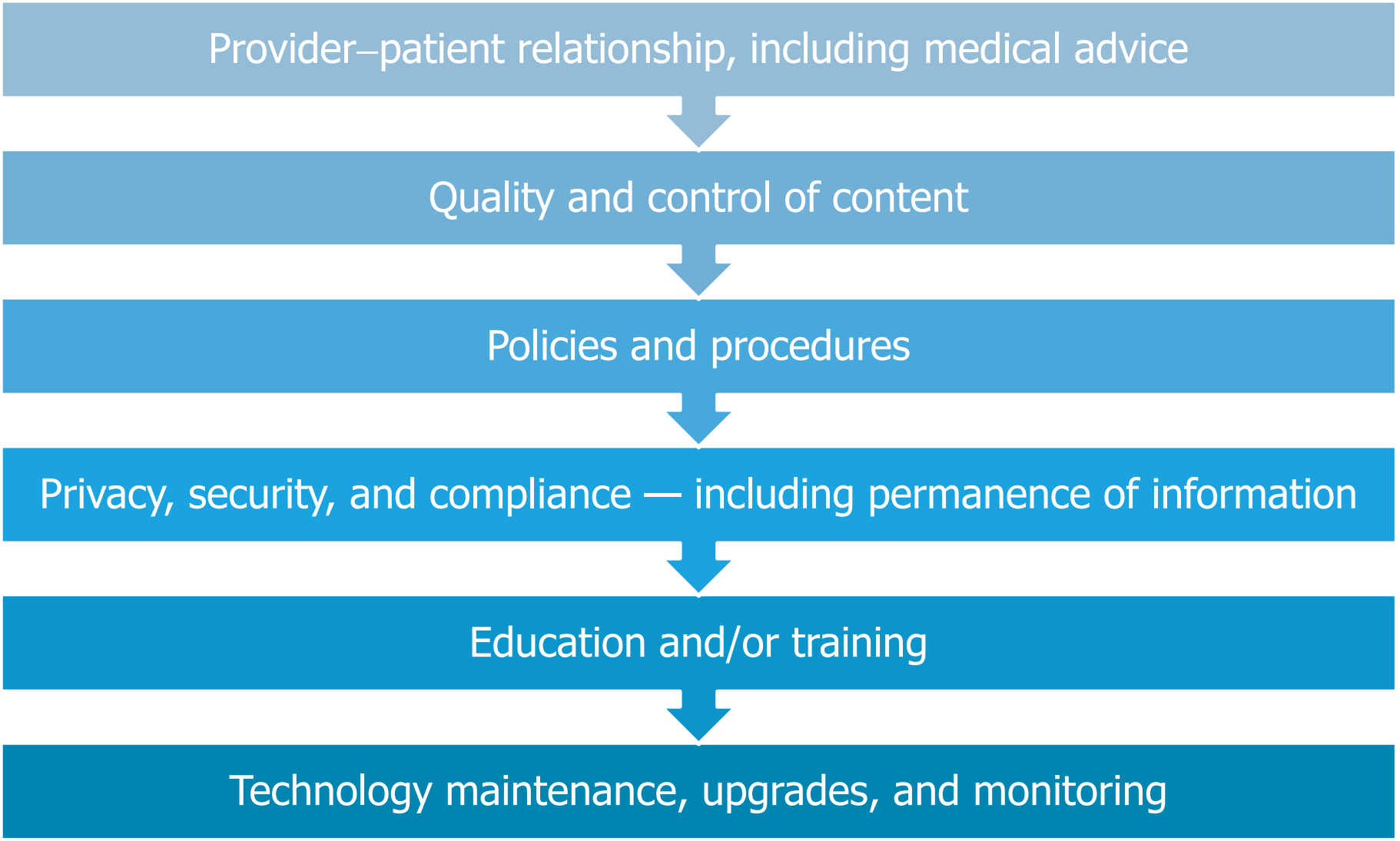
Risk assessment process after a breach

Minimally, four factors must be considered in the risk assessment:

- The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification
- The unauthorized person(s) who used the PHI, or to whom the disclosure was made
- Whether the PHI was actually acquired or viewed
- The extent to which risks associated with the breach have been mitigated

Technology, communication, and documentation

Key risk areas



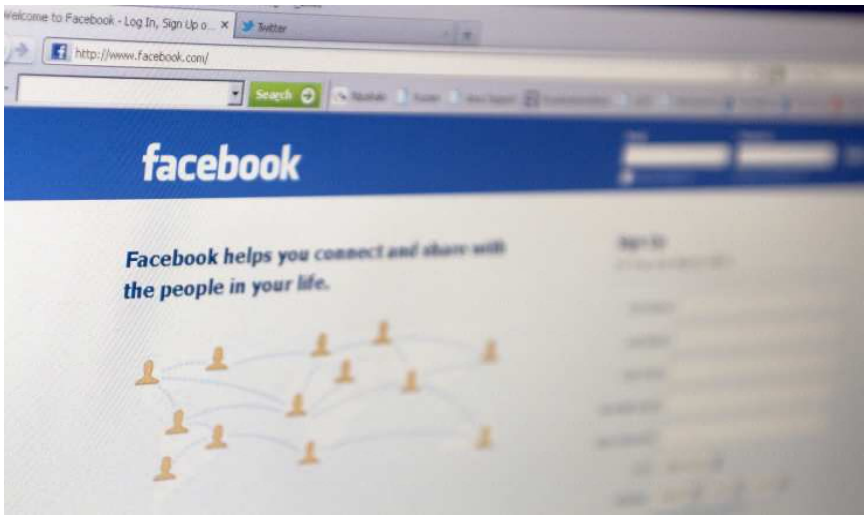
Use of social media in communication

- Quick dissemination of information
- Utilizes contemporary marketing methodologies
- Mechanism for reaching a tremendous number of people
- Recruiting and background checks
- Development of personal support and information-sharing groups

What about online reviews of your practice?

Options to consider:

- Do nothing.
- Ask the webmaster to remove the post.
- Do NOT engage in an online debate!



- If you do respond, do not respond to online comments. It's okay to script language to indicate you are committed to providing excellent patient care and encourage anyone with concerns to contact your office directly.

Email checklist

Do you have a signed release and acknowledgement from the patient that includes:

- ❑ Requirement that for emergent or urgent concerns, communication will be via phone or in person?
- ❑ Notice of the provider's right to refuse to make decisions or conclusions based on information obtained online?
- ❑ Notice that email communication is retained in the patient's healthcare record?
- ❑ Notice that the patient has read and accepted the practice's "online patient policies," which include hold harmless language and terms of use?
- ❑ Email server encryption requirements, and a waiver if patients opt not to use an encrypted service?

Case study — Texting

Scenario	Academic medical center used smartphones to enter orders.
Case Overview	Resident was in the process of discontinuing warfarin; at the same time, she received a party invitation via text message. The disruption caused her to forget to discontinue the medication.
Outcome	Three days later, the patient had a bleeding crisis that required surgery.
Key Issue	Did personal use of mobile technology cause the distraction, which resulted in the adverse outcome?

Risk issues with text messages

- May reside on a mobile device and with a carrier indefinitely
- Potential for exposure to unauthorized third parties due to theft, loss, or recycling of the device
- May be accessed without any level of authentication
- Interception and decryption of text messages possible with inexpensive equipment
- Information outside the health record

Risk mitigation for texting

- Establish a policy that prohibits or limits texting and establishes retention guidelines
- Train providers and staff on appropriate use
- Conduct inventory of all mobile devices, including personal
- Protect ePHI through passwords and encryption on all devices
- Delete data completely prior to retirement of any device
- Require health record annotation if texting is used for decision-making

Electronic Health Records

- EHRs — although intended to enhance communication and documentation — also are fraught with risks, such as:
  - System interface issues — hardware, software applications, data flow (i.e., between order entry and pharmacy)
  - Clinician communication pitfalls — including problems sending and receiving referral/consult information, as well as possible uncertainty as to whether the information was received
  - Overuse or inappropriate use of the cutting and pasting function
  - Alert fatigue
  - Process lapses, such as failure to review information for content and accuracy prior to finalizing documentation

EHR risk strategy

Identify functions within the EHR that create high risk for your practice, such as:

- Test tracking
- Drug interaction and allergy alerts
- Cancelled appointments and "no shows"
- Medication prescribing process

Consider developing a performance improvement plan to help mitigate these risks.

Patient portals

- Secure online website giving patients 24-hour access to PHI, including:
  - Prescription requests
  - Discharge summaries
  - Diagnostic test results

- Terms of use should be clear
- Access should be via encrypted, password-protected login process
- EHR audit trail should be utilized — validate who accessed patients' records and when
- Goal should be to enhance provider–patient communication and to improve patient outcomes

http://healthit.gov/providers-professionals/faqs/what-patient-portal

Telemedicine

Definition of telemedicine

"Telemedicine is the use of medical information exchanged from one site to another via electronic communications to improve a patient's clinical health status.

Telemedicine includes a growing variety of applications and services using two-way video, email, smartphones, wireless tools, and other forms of telecommunications technology."

American Telemedicine Association. (n.d.). What is telemedicine? Retrieved from http://www.americantelemed.org/about-telemedicine/what-is-telemedicine

Telemedicine — considerations

- When to see patients via telemedicine technology
- Scheduling
- Guidelines for patients on how to use the technology
- Systems must be HIPAA-compliant
- Licensing
- Provider reluctance to use
- Reimbursement
- Informed consent

Crane, M. (2014, July 25). Exploring telehealth models. Medical Economics, 91(14), 17–20. Retrieved from http://www.modernmedicine.com/sites/default/files/images/digital/ME/me072514_ezine.pdf

Risk issues

Clinical

- Provider–patient Relationship
- Patient assessment
- Medical advice
- Patient education

Admin

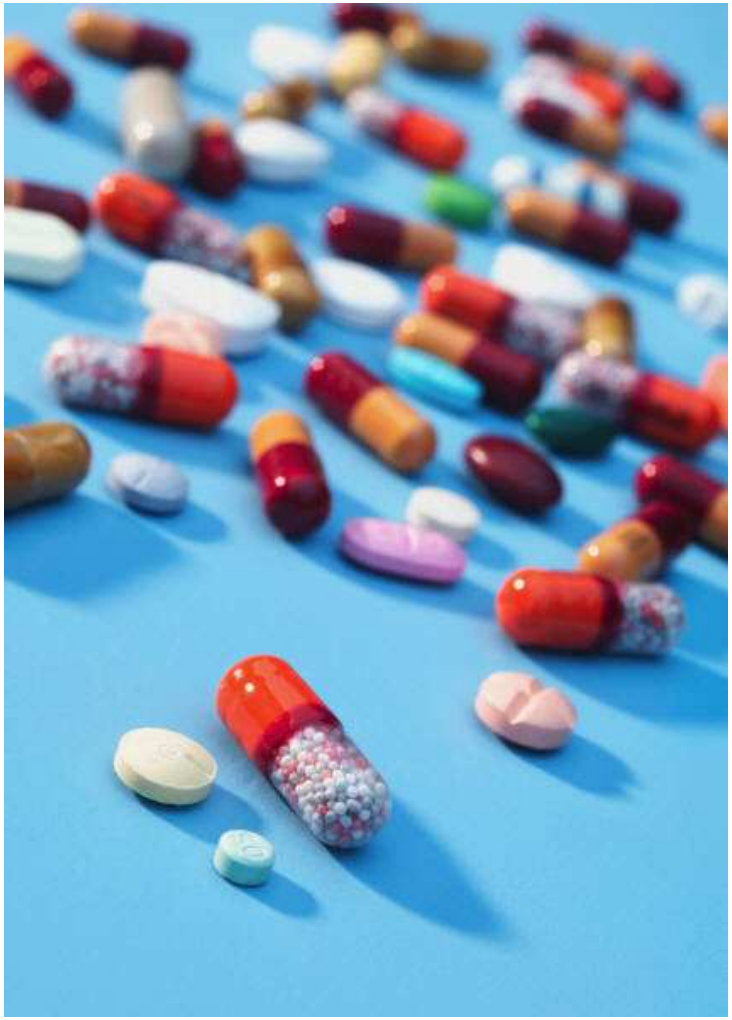
- Documentation
- Billing
- Patient identification
- Privacy/security
- Maintenance of technology

Regulatory

- State and federal regulations
  - Informed consent
  - Clinical decision-making
  - Quality improvement
  - Written agreements, MOUs, contracts

Online prescribing

- Provider–patient relationship
- Adequate physical exam
- Accuracy of patient history
- State licensing board requirements
- Federal regulations
- Majority of legal actions that have been brought against telehealth providers are related to online prescribing



Informed consent

- Telemedicine-specific:
  - Names of all involved healthcare providers, as well as credentials and location
  - Plan for ongoing care (who is responsible)
  - Security/privacy measures
  - Risks associated with use of telehealth services (e.g., technical problems)
  - Alternative plan in case of emergency/malfunction

- Should be documented in the patient's medical record

Privacy/security of PHI

- Transmission of data for telehealth services must comply with HIPAA and HITECH standards, as well as any relevant state laws (same duty as in-person care)
- Safeguards must be in place at every point in the process (originating site, transmission medium, distant site).
- Providers must be aware of approved vs. nonapproved technologies for telehealth
- Policies/protocols for confidentiality

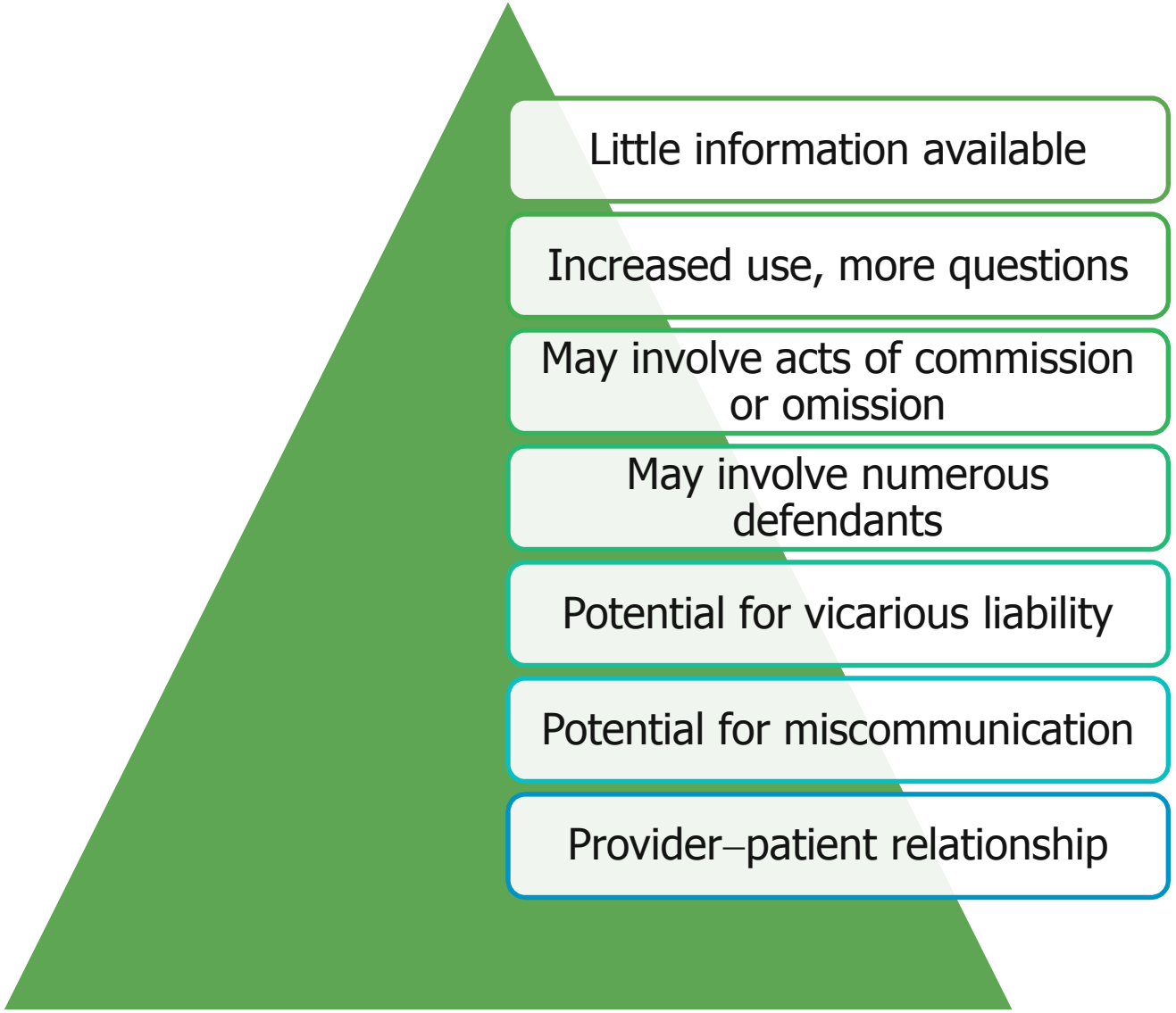
Risk strategies

- Ensure that telehealth providers are properly credentialed.
- Ensure that communication from telehealth providers is promptly reviewed and acted upon.
- Develop and implement standardized clinical protocols.
- Ensure that complications and adverse events associated with telehealth services are reported as part of the practice's incident report policy.
- Gauge patient and provider satisfaction with telehealth program using surveys or questionnaires.

Risk strategies

- Ensure that technology used to facilitate telehealth interactions is functional and used appropriately by providers and patients.
- Follow available telehealth standards to reduce risks of error and lost data.
- Provide staff training on telehealth technologies, scope of service, maintenance, and policies/protocols.
- Understand the requirements related to the telehealth technology being used.
- Implement privacy and security safeguards for the transmission of patient health information.

Malpractice liability



New technologies

- **Embrace or avoid?**
- **Where are you on the adoption continuum?**
- **If you take the leap, do your due diligence!**

Pressure to purchase and use new technologies

- Increase revenue/profit
- Competitive advantage
- Appeal for younger doctors, staff
- Patient demand and growing market pressure
- Marketing that overpromises results but fails to define risks

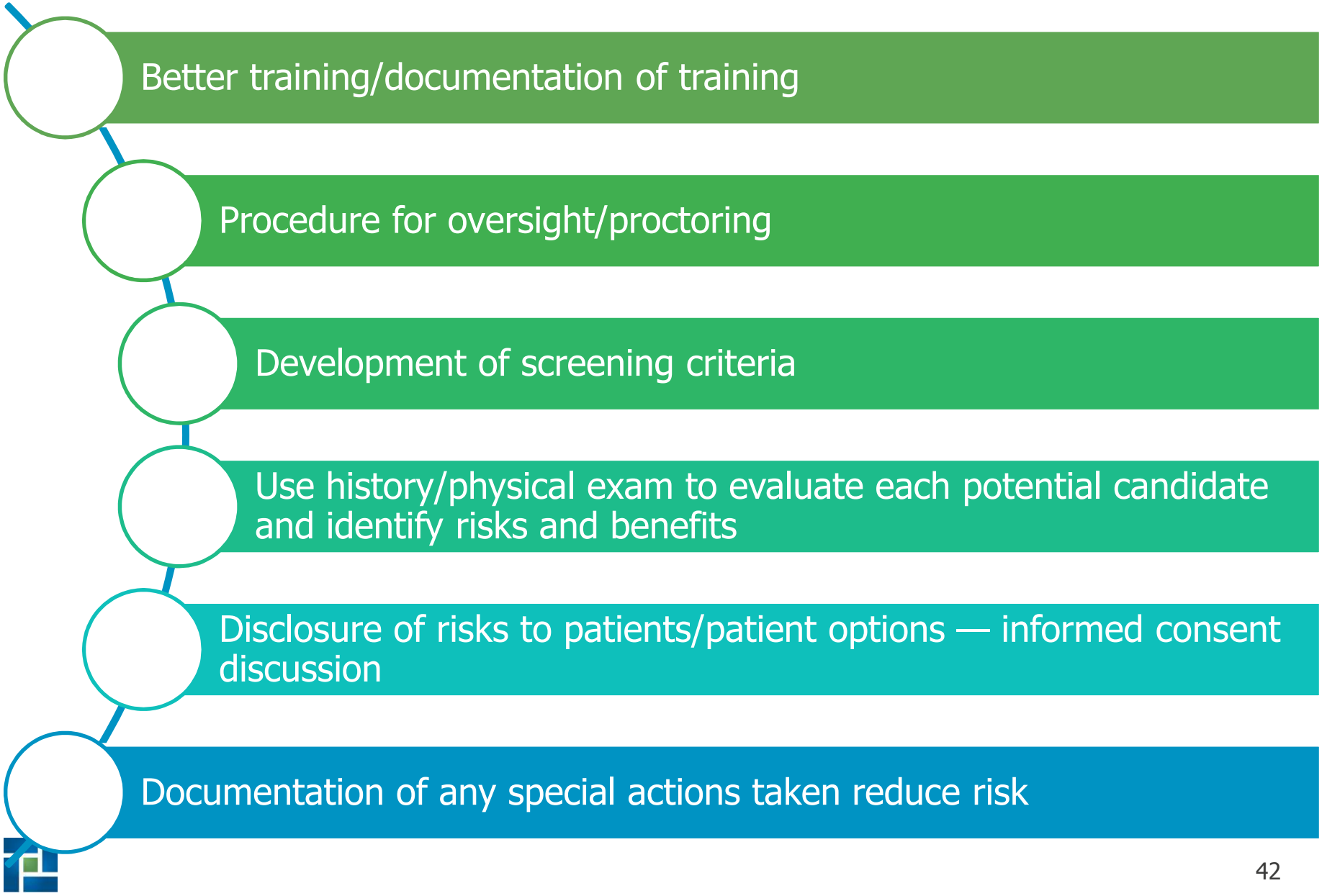
General risk management concerns

- Lack of awareness regarding learning curve, path to proficiency (volume)
- External pressures, i.e. patients, hospitals, etc.
- Patients unaware of risks, lack of informed consent
- Overestimation of benefits
- No universally accepted guidelines on how to train or length of training
- Because the technology is so new, standards of care have not yet been established

Training, competency, and credentialing

- Initial training for doctors and staff
- Proctoring/oversight
- Proficiency — How many is enough?
- Credentialing
- Ongoing training and competency testing

Risk strategies



Due diligence and planning before implementation

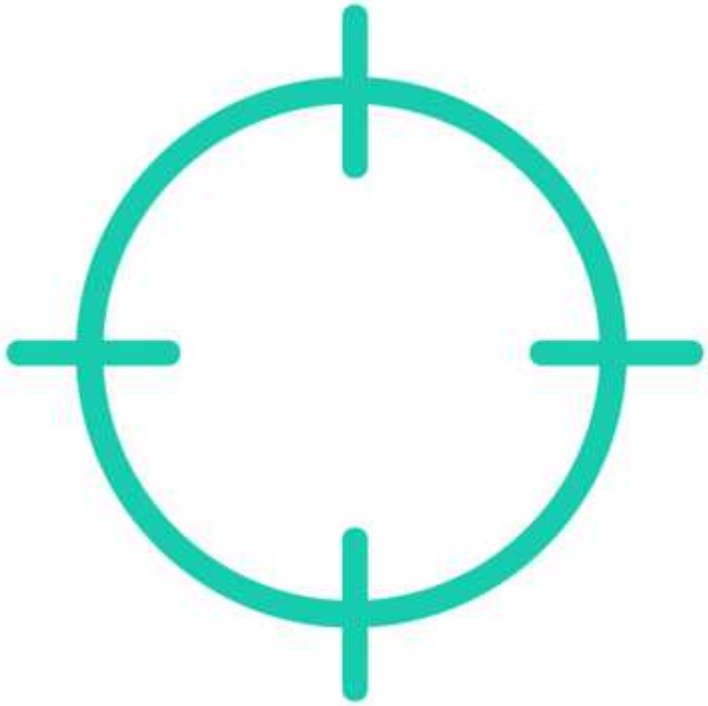
- Is your entire team (staff, office, etc.) on board with implementation of this new technology?
- Will this technology help you move forward, i.e., increase market visibility, enhance encounters with your patients, streamline communication?
- Were all end-users involved in the decision-making process?
- Does this technology blend in well with existing policies/procedures (e.g., social media policy, patient portal access, etc.) or will new policies and procedures need to be developed?

Final warnings

- Pause, think, and think some more about use of various technologies in your practice.
- Patient perception is the foundation of litigation.
- The only thing that lasts forever is electronic media.
- The only thing that doesn’t last forever is electronic media that can’t be preserved.

The joy of technology

Technology is a moving target.



In the time it took us to present this program, telemedicine evolved in another new direction.

What questions do you have?

Disclaimer

The information contained herein and presented by the speaker is based on sources believed to be accurate at the time they were referenced. The speaker has made a reasonable effort to ensure the accuracy of the information presented; however no warranty or representation is made as to such accuracy. The speaker is not engaged in rendering legal or other professional services. If legal advice or other expert legal assistance is required, the services of an attorney or other competent legal professional should be sought.