HIMSS MIDWEST AREA Chapters

FALL TECHNOLOGY CONFERENCE
MIDWEST


2012 Midwest HIMSS
Fall Technology Conference
"Field of Dreams"
If we build IT...They will come

# Privacy and Security Risks and Requirements with Healthcare IT:

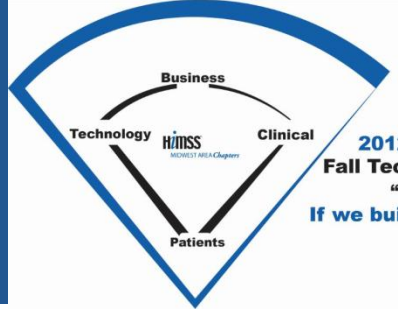
## Hitting a Home Run Instead of a Foul Ball

*Presented by:* *Sara Anne Hook, M.B.A., J.D.*
*Professor of Informatics*

November 2012

Leadership Track - Session #4C

HIMSS MIDWEST AREA Chapters




2012 Midwest HiMSS
Fall Technology Conference
"Field of Dreams"
If we build IT...They will come

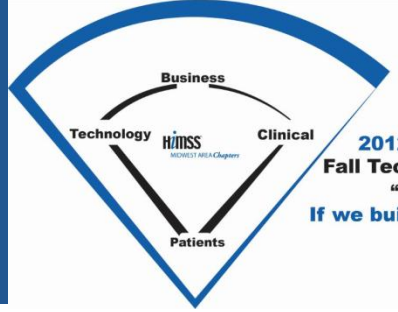
# Conflict of Interest Disclosure

**Sara Anne Hook has no real or apparent conflicts of interest to report.**
**Josette Jones has no real or apparent conflicts of interest to report.**

**Slides prepared by Sara Anne Hook, M.B.A., J.D. and Josette Jones, Ph.D., R.N.**

HIMSS MIDWEST AREA Chapters

# Abstract




2012 Midwest HiMSS
Fall Technology Conference
"Field of Dreams"
If we build IT...They will come

Using baseball as a metaphor, this practical, engaging session will explore the security and privacy risks with a number of technologies for storing, handling and communicating health information.

It will also highlight the legal obligations and technological requirements for collecting, preserving and producing health information as part of an electronic discovery process.

HIMSS MIDWEST AREA Chapters


# Electronic Discovery

HIMSS
MIDWEST AREA *Chapters*

# New Rules of the Game in Discovery


In the context of health IT, the emphasis is typically on maintaining the confidentiality of health information through proper security and privacy measures, absent either the patient's consent or as necessary for the provision and payment of health care services.

However, there are times when health information must be properly collected, preserved and produced, typically as part of litigation, investigation or audit.

This phase of the legal process is known as discovery.

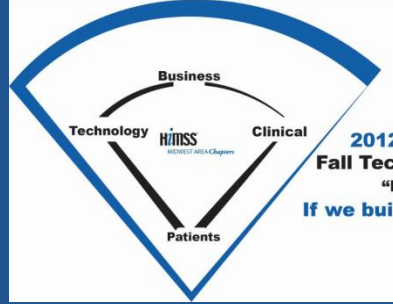
Famous legal cases (*Zubulake v. UBS Warburg*) and revisions to state and federal rules of court procedure (Federal Rules of Civil Procedure 2007) and evidence (Federal Rules of Evidence) have resulted in an emerging area within law practice known as electronic discovery, or e-discovery.

We now have the term "Electronically Stored Information" – or ESI.

# New Rules of the Game in Discovery


- Electronically stored information – terminology intended to be broad and encompass current and future information technologies.
- Cast a wide net at the beginning of a matter.
- Wide net also on the duty to preserve ESI.
- "Such media include cache memory, magnetic disks, such as computer hard drives or floppy disks, optical disks, such as DVDs or CDs, and magnetic tapes."
- Anything that can be read through the use of computers.
- Social media.
- Email – and danger of waiving attorney-client privilege and attorney work-product protection .

# Knowing the New Rules of the Game: Why It Matters in Health IT?




2012 Midwest HiMSS Fall Technology Conference
"Field of Dreams"
If we build IT...They will come

•An organization that has the appropriate policies, procedures and technologies in place for collecting, storing and disposing of its information and can document their approaches has a better chance of responding to electronic discovery requests and in avoiding any claims for sanctions.

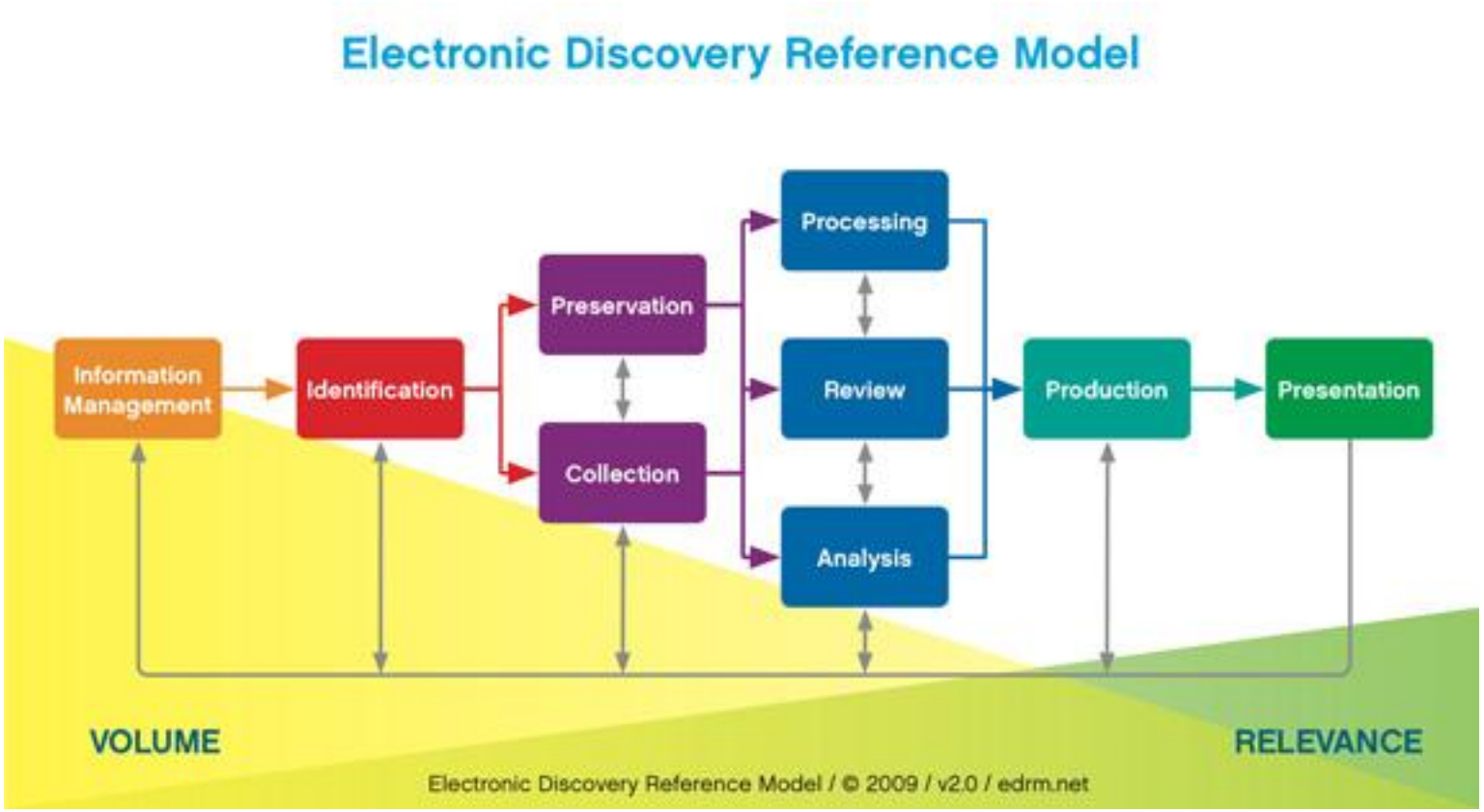
•Although the legal aspects of electronic discovery are primarily the purview of in-house and outside attorneys, readiness and the ability to respond to electronic discovery requests also require the participation of representations from clinical departments, management, IT, vendors and, human resources.

•Need to consider the lifecycle of information.

•Need for a Document Retention and Destruction Program – and be able to demonstrate that it is followed (in order to claim Safe Harbor Provision).

# Electronic Discovery Reference Model (EDRM): Field of Play






EDRM, www.edrm.net, accessed 11/5/12.

# Potential E-Discovery Foul Balls


- The multitude of places where ESI may be stored – not just a file cabinet
- The ongoing duties of counsel, especially with respect to issuing and overseeing litigation holds.
- The sheer volume of material that must be preserved and reviewed prior to production.
- The risk that information that could have – and should have - been protected under the attorney-client privilege or another doctrine of confidentiality, such as physician-patient, will be inadvertently produced.
- The expense of the electronic discovery process, especially when thinking about parties that may be non-profit hospitals or health care facilities.
- Note that the first step in the EDRM is Information Readiness: within the responsibilities of health IT staff and something that all organizations can do.
- Concept is zero minus one – in other words, responsibility for collecting and preserving ESI begins when there is a reasonable anticipation of litigation (audit, investigation, etc.), not when a summons or letter is received.

# Potential E-Discovery Foul Balls


- Native versus image formats - spreadsheets and databases as example, to allow the requesting party to conduct searches and analysis.
- The increasing harshness of sanctions for spoliation and for failure to participate in good faith in the development of an electronic discovery plan.
- The reality that many attorneys are not prepared for – or even aware of – electronic discovery.
- New training and certification opportunities – may need to hire people with this expertise (computer forensics).
- The fact that the electronic discovery industry as a whole is still in its infancy – with many more robust technologies still to be developed (predictive coding now permitted, machine-assisted review using algorithms built from keywords).

# Potential E-Discovery Foul Balls


- Portable devices, home computers, text messages, etc.
- Email messages – note cases where attorney-client privilege waived when using employer's email system and employer maintains right to monitor (also home email where shared or accessed by family members).
- Other places where information might be located that counsel, administrators, patients, health IT staff may not even think of (photocopiers, digital cameras, flash memory, CDs, cloud storage, smartphones, databases, DropBox, GoogleDocs).
- Also need to preserve information on websites.
- Although The Sedona Conference and other groups have attempted to outline best practices, there is still no standardized approach for how to handle an electronic discovery process.
- Parties may be ill-prepared to deal with an electronic discovery process, especially patients, physicians and health IT staff members.
- Social media – nearly 100% discoverable (even in criminal law cases) and nearly always admissible in court.
- Alterations to data (intentional versus negligent) may result in a claim of spoliation, resulting in sanctions.

# Potential E-Discovery Foul Balls

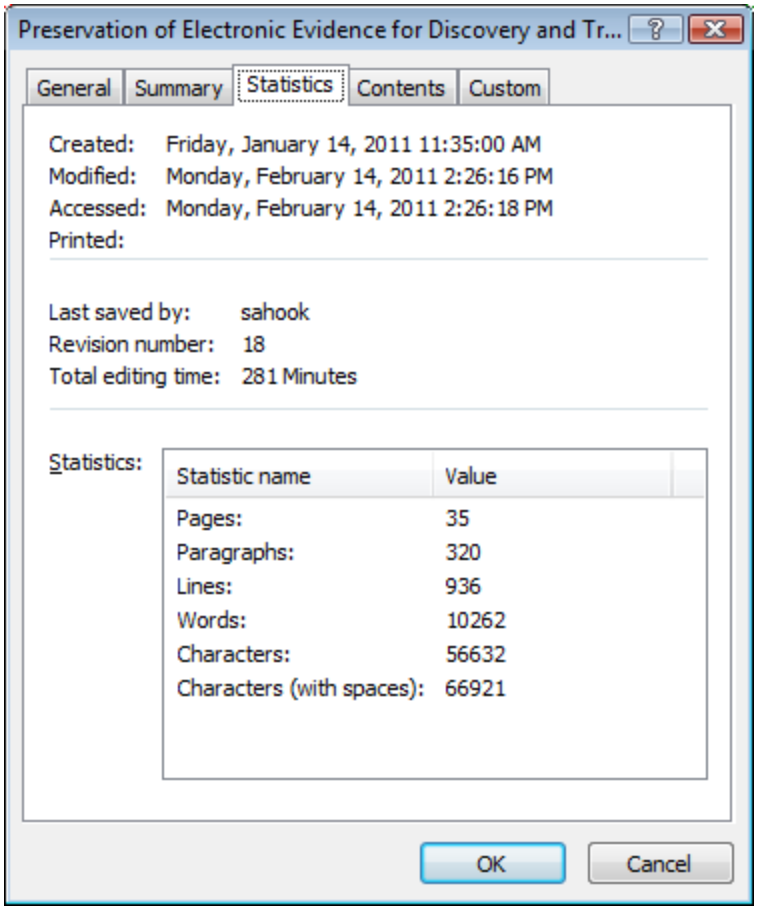

- Electronically stored information is fragile and can be altered even by booting up the computer.
- There may be a lack of clarity on some issues, such as when information is reasonably accessible versus when it is inaccessible.
- The decision on how much of an electronic discovery process should be handled in-house by the party versus outsourced to an electronic discovery vendor – and the selection and ongoing oversight of that vendor .
- Puts health IT staff in an awkward position – may not be prepared for the rigorous data collection processes and takes away from daily responsibilities. Also presents a conflict of interest for the employee (tendency or pressure to protect the employer).
- Dealing with legacy data systems.

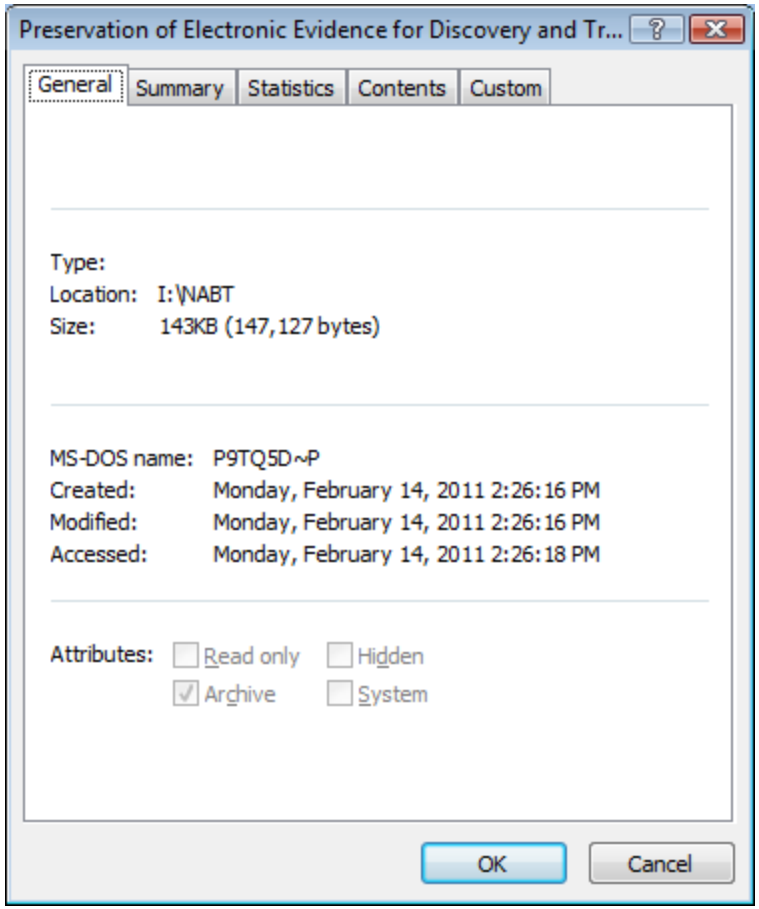
# Potential E-Discovery Foul Balls


- Metadata and the duty to preserve it in a way that links it with its corresponding files.
- Mirror imaging as the preferred approach.
- The opportunity to use sampling and testing.
- The requirements for a meet-and-confer conference and for opposing counsel and parties to cooperatively develop an electronic discovery plan.
- Safe harbor provision – hospital or health care facility must have a document retention and destruction policy that it is following consistently.
- Clawback and quick peek agreements.
- The short timelines and deadlines for some of the requirements in an electronic discovery process – results in privileged materials slipping through the review process and being produced to the opposing party.
- Ethical issues - attorneys, health care professionals.

# Metadata: Example from MS Word



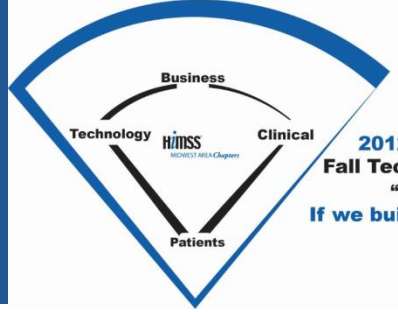


# Old Rules of the Game Still Apply


- Before ESI that has been produced can be presented in court, it still must comply with the Rules of Evidence:
  - Relevant
  - Responsive
  - Best evidence rule
  - Authentication
  - Hearsay
  - Judge's overall discretion – prejudice versus probative value, cumulative, etc.
  - Expert witness – computer forensics expert testimony may include methodology, chain of custody, use of mirror image
- Proportionality argument in ESI requests.
- Cost-shifting allowed, especially for third-party requests (traditional rule is that the producing party pays).

# Sanctions: You Struck Out!




2012 Midwest HiMSS
Fall Technology Conference
"Field of Dreams"
If we build IT...They will come

- Failure to comply with the requirements in an electronic discovery process has resulted in significant sanctions for parties as well as their attorneys.
- Money damages are increasing. Million dollar damages are not unheard of.
- Several years since 2007, when the Federal Rules of Civil Procedure were amended.
- Judges are increasingly savvy with technology and with the application of the rules.
- Other sanctions on parties: adverse inference instruction, costs of re-doing collection and analysis processes, need to hire expensive consultants and experts, court costs, attorney fees, dismissal of case.
- Bad publicity for the health care facility, health care provider, health IT staff.

# Recent Health Cases: You Be the Umpire!


- *Gaalla v. Citizens Medical Ctr.,* 2011 WL 2115670 (S.D. Tex. May 27, 2011).
- *Lowy v. Peacehealth*, 280 P.3d 1078 (Wash. 2012).
- *Estate of Wilson v. Addison*, 258 P.3d 410 (Mont. 2011).
- *Squeo v Norwalk Hosp. Assoc.*, No. CV095012548, 2011 WL 7029761 (Conn. Super. Ct. Dec. 16, 2011) and *Squeo v. The Norwalk Hosp. Assoc.*, 2010 WL 5573755 (Conn. Super. Ct. Dec. 14, 2010). (unreported decisions, subject to further appellate review).
- *Gotlin v. Lederman*, 2010 WL 2843380 (E.D.N.Y. Sept. 1, 2009).
- *Brown v. Coleman*, 2009 WL 2877602 (S.D.N.Y. Sept. 8, 2009).
- *Cornwell v. N. Ohio Surgical Ctr.*, 2009 WL 5174172 (Ohio Ct. App. Dec. 31, 2009).
- *Kilpatrick v. Breg, Inc.,* 2009 WL 1764829 (S.D. Fla. June 22, 2009).

# More Cases: Don't Throw the Bat!


•Scott v. Beth Israel Med. Center Inc., 2007 WL 3053351 (N.Y. Sup. Ct. Oct. 17, 2007). (loss of attorney-client privilege when user employer's email system)

Recent cases and a Formal Ethics Opinion from the American Bar Association demonstrate that the attorney-client privilege can be inadvertently waived by communicating with the attorney through an email system that third parties can access. The most common examples are using an employer-provided email system ,where the employer retains the right to monitor, or a family situation, where family members either allow each other to access their email messages or log into the email system using the same credentials.

•*G.D. v. Monarch Plastic Surgery, P.A., 2007 WL 201154 (D. Kan. Jan. 24, 2007).* (improper disposal of computer – placed on the curb for the trash)

Research shows that nearly 70% of computers donated to charity still had personal information stored on them.

# E-Discovery: Swing and a Miss


From this small sample of cases, it is clear that electronic discovery is an issue for any organization that creates, stores, manages and uses health information.

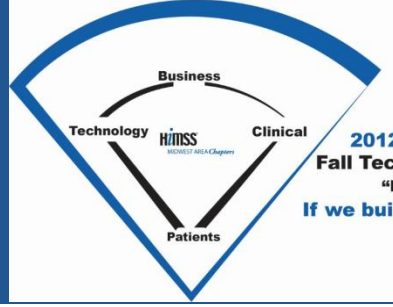
These cases also illustrate the range of swings and misses in the electronic discovery process in health care:

Sanctions, back-up tapes, spoliation, records retention policy, data preservation, personal computer, social media, email, lack of cooperation in electronic discovery process, "nonfunctional" hard drives, keyword searching, forensic experts, mirror image, foreign language documents, reasonably accessible, relevance, attorney-client privilege, inadvertent disclosure, improper disposal of computer equipment.

These cases involve medical malpractice, wrongful death, breach of contact and wrongful disclosure of medical information.


# Security and Privacy Risks

# Technology Risks: Foul Balls



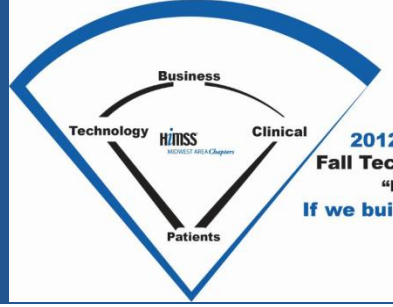

2012 Midwest HiMSS
Fall Technology Conference
"Field of Dreams"
If we build IT...They will come

•The technologies that may represent foul balls - and even strike outs - in the privacy and security of health information arena are:

- •social media
- •cloud computing
- •mobile and wireless devices
- •information storage practices

•An especially risky approach for collecting, processing and maintaining health information is the increasing trend towards outsourcing these functions, especially by using third-party vendors who are not located within the boundaries of the United States and thus not subject to U.S. laws regarding the use of appropriate privacy and security practices.

# Privacy and Security Law: Faulty Rulebook



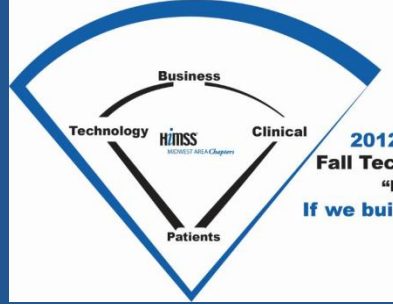



Concerns with privacy and security of all types of information have resulted in a patchwork of state and national laws intended to address global issues and specific situations.

Recent examples:

- The prohibition on the use of social security numbers.
- The requirement of redacting certain categories of information from court documents.
- The recent furor over requests for Facebook passwords from job applicants.
- Warrantless surveillance using various devices.
- DNA database of samples from arrestees.

# Social Media: Foul Balls




2012 Midwest HiMSS
Fall Technology Conference
"Field of Dreams"
If we build IT...They will come

•Although social media offers powerful opportunities for health education and outreach, it presents special risks as well.

•The tendency for spontaneous over-sharing of information may mean a breach in the confidentiality of a patient's information that would result in claims against the health care provider and his/her employer.

•It can also be a breach in a health care professional's ethical duties in addition to being grounds for disciplinary action from the employer and a lawsuit by the patient.

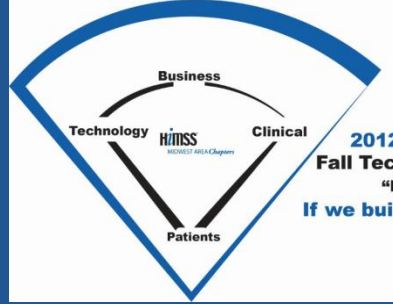
# Social Media: Foul Balls


•As stated in the abstract to the article by Hader and Brown, "[h]ealthcare providers using social media must remain mindful of professional boundaries and patients' privacy rights. Facebook and other online postings must comply with the Health Insurance Portability and Accountability Act of 1996 (HIPAA), applicable facility policy, state law, and AANA's (American Association of Nurse Anesthetists) Code of Ethics."

•As the authors note on page 273, "it is easy to see how a healthcare provider who posts work-related information online in a Facebook status update, a 'tweet,' or a discussion blog could unwittingly become ensnared in a disciplinary investigation at work, a federal investigation of a possible HIPAA violation, a disciplinary investigation by the state licensing agency, and a civil lawsuit filed by an aggrieved patient."

•They suggest that although new media tools serve important social and professional purposes in today's society, the most prudent course of action is to stop and think before posting.

# Social Media: Foul Balls

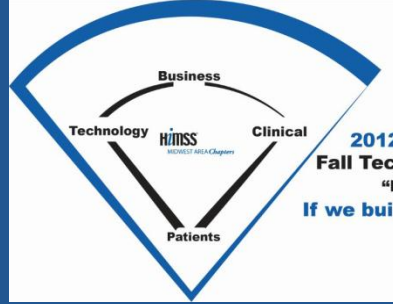



2012 Midwest HiMSS
Fall Technology Conference
"Field of Dreams"
If we build IT...They will come

•In their article, Greysen, Kind and Chretien state that the rise of social media has brought new hazards for medical professionalism. They assert that "[m]uch like a mirror, social media can reflect the best and worst aspects of the content placed before it for all to see."

•Among the issues they discuss are that physicians do not consider the potential impact of their online content on patients and the public and that a momentary lapse in judgment by an individual physician who posts unprofessional content on social media leaves a digital footprint that may cast the entire profession in an unflattering light.

# Social Media: Foul Balls



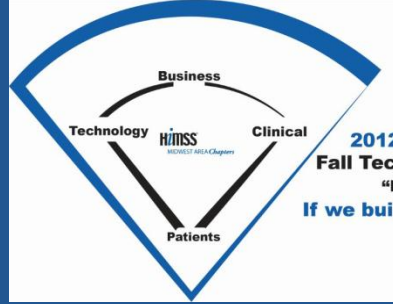

2012 Midwest HiMSS
Fall Technology Conference
"Field of Dreams"
If we build IT...They will come

It's not just about privacy of patient information.

Nelson and Simek also identify other risks with social media:

- Adverse publicity
- Misleading advertising
- Unvetted postings
- Undisclosed endorsee connections and conflicts of interest
- Illegal employment practices

# Social Media: Call the Play



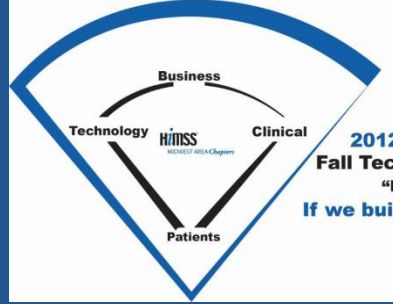

2012 Midwest HiMSS
Fall Technology Conference
"Field of Dreams"
If we build IT...They will come

•Revisions to an employer's Acceptable Use policies- should also include email, Internet, telephone, any employer-provided information technology as well as social media, blogging, tweeting, YouTube.
•Caution health care providers, other staff members, volunteers, about inadvertently sharing patient information through social media
•Caution patients and family members about inadvertently sharing patient information through social media

•Recommended by Nelson and Simek:

•Monitor employee activity on social media.
•Provide strong consequences and make them clear.
•Impose technology controls.
•Create a media czar position.
•Balance social media potential against risks.

# Social Media: Call the Play



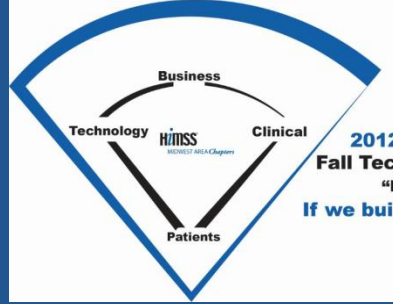

2012 Midwest HiMSS
Fall Technology Conference
"Field of Dreams"
If we build IT...They will come

According to Nelson and Simek, the major elements of a social media policy are:

1. Address all potential pitfalls in a clear and organization-specific manner and be consistent with other organizational policies and procedures.
2. Distinguish between business and personal use (on-the-job and off-the-job conduct).
3. Inform employees of the rules and regulations that state that they will have a reduced or non-existent expectation of privacy on any of the organization provided computers, e-mail systems, mobile devices, and telephone or voicemail systems.
4. Encompass what can be said, who can say it, and the manner in which things should be said.

The policy should limit who has the authority to speak on the organization's behalf, including the use the organization's name and its logos, trademarks or copyrights.

# Social Media: Call the Play




2012 Midwest HiMSS
Fall Technology Conference
"Field of Dreams"
If we build IT...They will come

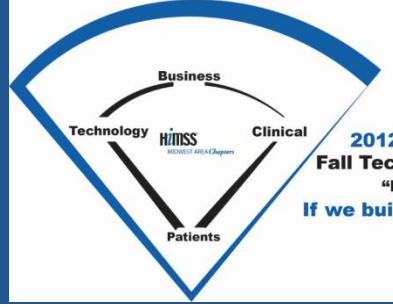
Other advice from Nelson and Simek (from *Mitigating the Risks of Using Social Media*, Sensei Enterprises, 2011):

An organization's policy should provide a clear explanation of what an employee is permitted and forbidden to say. Addressing content that can be posted on social media sites can prevent a variety of mishaps, including:

- Preventing the inadvertent posting of confidential information and trade secrets.
- Curtailing defamatory or otherwise inappropriate content.
- Stopping any other unlawful of criminal information from being posted.

The policy should also instruct employees to avoid controversial, topics, to use a polite and respectful tone, even when disagreeing, and to never post anything that could conceivably be construed as discrimination, harassment, or defamation.

# Mobile Devices and Wireless: Foul Balls




2012 Midwest HiMSS
Fall Technology Conference
"Field of Dreams"
If we build IT...They will come

- Many health care institutions, practitioners and patients have embraced mobile devices for their convenient size and ready access to information.

- However, wireless networks can be notoriously insecure.

- Information on an iPad screen has been shown to be visible from several feet away [research by Jones *et. al*].

- Laptops and cell phones are frequently misplaced or stolen, putting any information stored on them at risk.

# Mobile and Wireless: Call the Play


- Kimbro devotes a number of sections of her book to such important topics as protecting client confidences, storage and retention of client data and securing mobile devices. (Kimbro, S.L. *Virtual Law Practice: How to Deliver Legal Services Online*. Chicago, IL: American Bar Association, 2010).
- Although intended for the legal world, they are also applicable to health IT.
- "Use full disk encryption on all computers.
- Create strong passwords. Change them occasionally. Make sure username and passwords are not written down or are not easily viewable or accessible.
- Use a daily backup system.
- Keep anti-virus software up-to-date and a firewall in place.
- Use anti-malware protection.

# Mobile and Wireless: Call the Play


- Use a pop-up blocker, depending on the browser you use. (Firefox is recommended with the use of security add-ons.)
- Have a secondary, backup Internet method, such as a wireless AirCard.
- Secure your wireless.
- Remove metadata before transmitting documents.
- Educate and remind your online clients about protecting themselves using their own hardware.
- Purchase insurance for hardware."

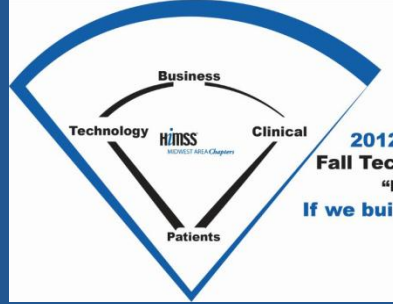
# Cloud Computing: Foul Balls


•Cloud computing presents some attractive benefits in terms of reducing IT hardware, software and personnel expenses.

•The risks of a breach in client confidentiality may increase with the greater use of cloud computing and third-party vendors that are used to provide software and maintain the law firm's information. (See *The Lawyer's Obligations When Outsourcing Legal Services and Nonlegal Support Services*, ABA Formal Ethics Opinion No. 08-451, August 5, 2008 (accessed July 19, 2008)).

•These same risks confront hospitals, health care facilities, health care providers and health IT staff when relying on cloud computing services and third-party vendors.

# Cloud Computing: Call the Play



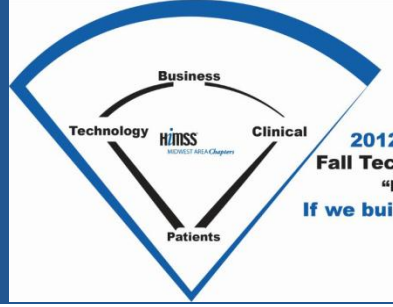

2012 Midwest HiMSS
Fall Technology Conference
"Field of Dreams"
If we build IT...They will come

•A well-drafted and comprehensive information security and privacy schedule is recommended as the first step in ensuring that confidential patient information is secure and handled in a manner that is in compliance with federal and state law.

•Among the issues to be addressed in any kind of cloud computing or outsourcing contract are the security assessment process, specific privacy and security controls, data retention, return and destruction, incident response planning, enforcement rights and liability and notification for security breaches.

•Be sure to read the contract for these services carefully, especially with respect to the security, access and confidentiality of information.

# Cloud Computing: Call the Play




2012 Midwest HiMSS
Fall Technology Conference
"Field of Dreams"
If we build IT...They will come

- Kimbro devotes an entire chapter of her book to choosing technology, including cloud computing and Software as a Service (SaaS).
- "Research the software provider and hosting company.
- Downtime for maintenance or upgrades
- Support for future law office growth
- Cost of the product
- Data return and retention policies
- Third-party hosting
- Offshore servers
- Geo-redundancy
- Data escrow
- Compliance with federal regulations
- Liability for confidentiality breaches
- The provider's Service Legal Agreement (SLA)" (See Kimbro, pp. 39-65)


# I hope you have many Home Runs in Your Health IT!

HIMSS
MIDWEST AREA *Chapters*


# Any questions?

HIMSS
MIDWEST AREA *Chapters*