NORMAN HANSON DETROY

Portland Office: (207) 774-7000
Lewiston Office: (207) 777-5200

Experienced. Efficient. Effective.

News

Pitfalls in Using Nonprofits as a Return to Work Option

By Lindsey M. Sands

A key method to reduce exposure on any claim following a work-related injury is to be able to provide the injured employee with accommodated work. This option, when feasible, benefits all involved. It allows employers to limit indemnity costs associated with any injury while getting necessary work done. It also provides earnings to employees all while assisting in faster recoveries with less risk of deconditioning and psychological setbacks which are common for employees who are out of work indefinitely. However, often an employer does not have the ability to bring back a worker to perform necessary work within the employer's organization. For such cases, a crop of third party services have emerged which provides "transitional employment programs" in which employees are placed in either jobs which are not open to the general public or volunteer programs. In both cases, the employer pays the employee to simply keep them acquainted with work experience and in touch with the daily work routine.

These services can still benefit both employers and employees. However, there are risks involved in using such services in the context of litigation as a means to limit an employee's entitlement to workers' compensation benefits. The potential risk was recently highlighted by a case before the Appellate Division, Sylvester v. Marco Petroleum Industries, App. Div. Dec. No. 16-16. Mr. Sylvester was receiving total incapacity benefits per Decree when the employer offered to pay the employee $7.50 per hour to volunteer at Threads of Hope, a non-profit organization under the auspices of Catholic Charities of Maine. Mr. Sylvester accepted this offer and began to volunteer approximately six hours per week. The employer then filed a Petition for Review and Reduce Benefits pursuant to §205(9)(B)(2). After filing the Petition, the Employer reduced benefits based on receipt of the wages the employee was paid for volunteering at the non-profit. Mr. Sylvester then filed a Petition for Penalties with the Abuse Investigation Unit ("AIU") contesting the reduction of benefits and arguing that his income did not represent genuine wages. The employee specifically requested imposition of a fine in the amount of $200 per day pursuant to 39-A M.R.S.A. §324(2) for each day the employer/insurer was not paying him benefits reflecting total incapacity as set forth under the Decree.

The employee requested that the AIU Hearing Officer "take some testimony on this case or, based upon the written submissions, conclude that this is not a real job at all." According to Board Rules, the AIU will not allow testimony on a penalty proceeding absent "extraordinary circumstances." Citing this rule, the AIU Hearing Officer decided the case based upon written submissions and declined to impose a fine under §324(2). He found that the employer's unilateral reduction was proper "based on his earnings at Threads of Hope." The AIU Hearing Officer subsequently declined to issue further findings and the appeal to the Appellate Division followed. The Appellate Division vacated the underlying decision and remanded the matter back to the AIU for other evidentiary hearing, or an order staying the proceedings, until the Administrative Law Judge had decided the employer's pending Petition for Review.

As the Appellate Division pounced on a procedural error of the AIU Hearing Officer only, the case does not give guidance as to whether the employer's reduction of benefits based on Mr. Sylvester's "earnings" was appropriate or not. This case should, however, serve as a reminder to employers as to the risks and potential for litigation when using nonprofit providers as de facto return to work options. Litigation is ripe if the return to work offer is merely a sham with no genuine work being performed.

The Law Court further limited the use of these transitional work assignments in the case of Avramovic v. RC Moore

Transportation, 2008 ME 140. In Avramovic, an employer used a vendor to basically create a job for the injured worker. When the injured worker refused the job, the employer argued in favor of forfeiture of benefits for "refusal of a bona fide offer of reasonable employment." The Hearing Officer (now referred to as an Administrative Law Judge) found that forfeiture was not appropriate as the record included "very little evidence offered" about the job or what the employee would be doing. He further found that the employer did not prove that "the position offered is one that is actually available in the competitive labor market." An appeal followed and the Law Court upheld this finding. Avramovic establishes that created jobs and/or assignments which provide no benefit to the employer will not be considered the equivalent of real work for purposes of the forfeiture provision under 39-A MRSA §214(1)(A).

This does not mean that any such program should be viewed as useless. As noted above, there are certainly benefits both mental and physical to providing these accommodated work options. However, the employee's participation (or lack thereof) should not be used as the sole basis for pushing litigation. Moreover, such programs should be considered only when there is no viable return to profitable work with the employer.

Eyewitnesses Seldom Are

By Jonathan W. Brogan, Esq.

At trial no evidence is more compelling than that of an eyewitness. A person who was at the scene watching the events, hearing the cries of the injured and the crunching of metal, helping victims, guiding rescue worker is powerful and usually very convincing before any jury. Any experienced trial lawyer knows a credible and convincing eyewitness can establish or destroy a case.

Recently, I represented a client who was involved in an automobile accident on a major thoroughfare between Maine and New Hampshire. At the time he was traveling southbound from Wells, Maine, returning to his home in New Hampshire. Traveling in the opposite direction was a 103 year old gentleman who had just left his daughter's home in southern York County and was traveling northbound towards his home in Sanford, Maine. In front of him was a vehicle that was trying to make a left-hand turn. The older gentleman was driving a 4-door sedan. My client was driving a 4-door pickup. The older gentleman rear ended the woman making a left-hand turn causing a chain reaction accident which ended up involving, finally, four vehicles.

There were three independent eyewitnesses on the side of the road eating a piece of pizza at the convenience store that the turning woman was trying to enter. Unfortunately the older gentleman died as a result of the accident without making a statement about which way he was traveling. However, the testimony of my client was taken and he and his front seat passenger stated, truthfully, that they were traveling southbound. The family of the older gentleman testified that he had immediately left their home just before the accident and that his trip, if he was traveling as he should have been, could only have taken him northbound. The eyewitnesses testified that, in fact, all the vehicles were traveling in opposite directions to where they should have been.

At the deposition of the main eyewitness, a motorcyclist who was eating a piece of pizza at the side of the road, he was completely convinced that the truck driven by my client was traveling northbound. Despite being presented with undeniable evidence that he was incorrect, his memory was firm and his testimony was, in his mind, unshakable. Unfortunately, this is not an unusual event. Recently in a trial that I was defending, an eyewitness testified that the ambulance driven by my client was traveling without siren or emergency lights. At the trial, we

presented the testimony of the driver, two EMTs, and the patient in the ambulance involved in the accident. All testified that the lights were activated and the siren was working. The "eyewitness" stuck to her story despite conclusive proof that she was incorrect.

Justice Felix Frankfurter once said, "Identification testimony, even when uncontradicted, is proverbially untrustworthy." The criminal courts have long dealt with this issue and in fact the United States Supreme Court requires trial judges to assess the reliability of any eyewitness identification by applying a five factor test. Criminal defendants have been allowed to call expert witnesses to educate jurors on the scientifically proven perceptional difficulties of humans, especially under extreme stress.

Despite the known, and proven, fact that eyewitness testimony is intrinsically unreliable, most people, especially jurors, rely on eyewitness testimony at trial. The lawyer who is presenting that eyewitness testimony feels much more confident than the person having to cross examine that testimony even when it is patently unreliable. A famous jurist once wrote:

> The basic findings are: accuracy of recollection decreases at a geometric rather than an arithmetic rate (so the passage of time has a highly distorting effect on recollection); accuracy of recollection is not highly correlated with the recollector's confidence; and memory is highly susceptible – people are easily reminded of events that never happened, and having been 'reminded' may thereafter hold the false recollection as tenaciously as they hold the true one.

All of us are familiar with the difficulties that Brian Williams encountered in 2015 when talking about his "memory" problems. Though it made Mr. Williams the source of much derision, his same testimony, presented at trial, without refutation, would have been powerful and dispositive.

Scientifically, memory is a three stage process. First, there is perception. Perception, especially perception that takes place for a short time in an unfamiliar location in a moment of great stress, is highly suspect.

Once a perception is formed, every person then retains that perception in their memory. Unlike a photograph or a recording, a person's memory is not fixed at the time of the perception. In fact, memory is a malleable process subject to subsequent information and misinformation. In other words, a person who has a memory and begins to retain it, may have that memory changed by subsequent events, including interviews and suggestions. It has been shown through numerous tests that scientists can introduce misinformation to their subjects, destroying their memories, and creating, even in the strongest minded person, erroneous memories.

Time is also the enemy of eyewitness testimony. The further from the actual event, the less likely the person who perceived it will remember it accurately. However, anyone experienced with the trial process understands that people cling to their memories.

Permanent memories, which have been formed for years, are much more susceptible to memory illusions than recent memories. Memory illusions are the result of a human being's need to make sense of events. For instance, in the automobile accident case with the two vehicles traveling in opposite directions, the motorcyclist eyewitness was very influenced by the fact that the driver of the sedan that struck the turning vehicle was very elderly. It was clear he was trying to protect that gentleman and make his memory fit his belief that the older gentleman could not have caused the accident. The same was true with the ambulance case in which the eyewitness, who worked at a local bus station, saw emergency vehicles traveling through this very busy intersection near the hospital on many occasions and believed they did so without due regard for other vehicles. She also believed that this ambulance,

which because of the grave nature of the condition the patient within the ambulance, was ordered to leave the scene of the accident and go to the hospital, had obviously not been operating as it should have under the law. Therefore, at many trials we are confronted with witnesses who testify, honestly, as to what they thought happened even though it didn't.

Finally, the third stage of memory is retrieval. Each time a person is asked to remember an event, that event is retrieved and organized based upon the present situation of the eyewitness. If the eyewitness has to reconstruct the memory each and every time, the possibility of distortion is huge. Needless to say the same memory issues that can confront an eyewitness also confront jurors when they are evaluating the testimony of witnesses who are testifying at trial. The underlying biases and prejudices of jurors are meant to be discovered during voir dire, but jurors tend to believe fact witnesses who testify to what they saw, heard or felt in compelling detail even if that testimony has been shown to be incredible or lacking in truth.

Hundreds of criminal defendants have been convicted of crimes based on eyewitness testimony. It is only later that DNA testing shows that that eyewitness testimony was completely unreliable. In those situations, corroborating evidence is needed to break the jury from the belief that eyewitness testimony is infallible and must be believed at all times.

The best response to any eyewitness testimony that is irrational is to establish the basic underlying facts through corroboration. It is fascinating that even with the actual facts being established through corroboration that witnesses and their attorneys will still cling to the belief that a jury will reject the facts and accept the perception of an eyewitness, however tainted. More than once a trial has ended with the lawyer who had the better case finding that the jury did not believe his client because they believed the disputed and disproved eyewitness testimony. This is especially true in very emotional cases such as those involving the death of a highly susceptible victim (a child or an older person), a person claiming abuse at the hands of another or one claiming discrimination. It is important to remember that those kinds of highly stressful and difficult cases create in jurors the belief that they may have to "stand up" for the victim and therefore believe what they want to believe to do so.

In especially difficult eyewitness cases, behavioral and psychological experts can be employed to explain to jurors that humans are very prone to misperception of stressful events and that they overwrite their recollections of events with misinformation and are not "lying" when presenting these perceptions at trial. Obviously if a juror can be convinced by corroborating evidence and expert testimony that a sincere eyewitness is "sincerely" incorrect in their perception then that testimony is nullified.

W.C. Field famously said "there's a sucker born every minute". Someone once observed it is important to "tell them what they want and then give them what you tell them." In a trial situation, credibility is always crucial. An eyewitness, who will come into court, raise his or her hand, and relate what they claim they saw, is always difficult to refute. However, eyewitness testimony is highly unreliable and if it is the centerpiece of the opposition's argument, it must be refuted through corroborating evidence and, possibly, expert testimony regarding the unreliability of a person's memory. Though many don't want to believe it, most have had a Brian Williams moment. Nothing is more embarrassing then for someone's "recollection" to be pointed out to be wholly or partially false. Luckily most of us don't have network news shows and dozens of reporters recording our every move. However, reminding a juror of "Brian Williams moments" as well as the frailty of their own memory (how many of us have forgotten where are glasses are when they are still right on top of our head?) can be highly effective in helping jurors recognize that people make up stories for any number of reasons.

The criminal courts have recognized this problem and have instructions to deal with eyewitness testimony. In civil cases, however, the law still assumes that jurors and judges can tell fact from fiction. As we all know, that is not correct. Jurors need to be told, either through other testimony, expert testimony, and in instructions from the judge

that their daily experiences may not be the best preparation to evaluate the truth of eyewitness or memory based testimony and that the human memory is open to error at each of three stages or memory. Despite the jurors' belief, eyewitness testimony is often the worst kind of testimony, not the best.

New Federal Law Offers Different Avenue for Trade Secret Protection

Carl E. Woock, Esq.

In almost every industry, companies big and small rely on trade secrets to maintain an edge in a competitive marketplace. Trade secrets occupy a broad category of information that is commercially beneficial to a business and not generally known to the public. Some famous examples readily come to mind: the formula for Coca Cola or the secret behind the "nooks and crannies" in Thomas' English Muffins. Other trade secrets are more conventional (and less tasty): for example, a customer list for a Kennebunk plumbing company, purchasing information for a Bangor hardware store, or a consumer market analysis performed by a local credit union, all of which may be protected by trade secret law. Unlike patent, trademark, or copyright protections, which eventually expire, trade secrets last for as long as the secret is kept. Once that secret is lost, though, it is lost forever.

Until very recently, trade secrets were also different from trademark, copyright and patent law for another reason: trade secrets were primarily an object of state law. That is no longer the case. On May 11, 2016 President Barack Obama signed into law the federal Defend Trade Secrets Act of 2016 ("DTSA"). DTSA gives trade secret owners a new option to bring lawsuits for trade secret misappropriation using federal law and the federal courts. It has been called "most important piece of intellectual property legislation that Congress has passed in several years." That might overstate the law's significance, but this is certainly a development that businesses should take seriously.

What are the practical implications of this new law? Well, if a former employee marches over to a competitor with a confidential list of clients, a business owner might now bring a misappropriation of trade secrets claim in federal, rather than state, court. There are some conditions. The business can only make use of the federal remedies if "the trade secret is related to a product or service used in, or intended for use in, interstate or foreign commerce." DTSA uses an existing definition of "trade secret " from the Economic Espionage Act—that is, "all forms and types of" various categories of information, regardless of how stored, if "the owner thereof has taken reasonable measures to keep such information secret" and "the information derives independent economic value, actual or potential, from not being generally known" to the public. From there, the definition of "misappropriation" is borrowed from the Uniform Trade Secrets Act adopted in most states, primarily defined as the "acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means," or the "disclosure or use of a trade secret of another without express or implied consent by a person" who "used improper means to acquire knowledge of the trade secret." If these conditions apply to the employee hawking a confidential list of clients, federal remedies may be on the table.

Federal Remedies Are Both Familiar and New

DTSA largely tracks with the remedies provided by the Uniform Trade Secret Act. Specifically, DTSA's remedies include injunctive relief, actual damages, restitution, and exemplary damages of up to two times the actual damages, as well as attorneys' fees. In contrast to the uniform state laws, DTSA permits *ex parte* civil seizure of property to prohibit the dissemination of a trade secret without advance notice to the other side in "extraordinary

circumstances." If prosecuted by the federal government, an offender also faces penalties from $5 million to the greater of $5 million or three times the value of the stolen trade secret.

The headline, though, is that these remedies are available in federal court, which offers an intuitive upside. Without a uniform federal law, a company seeking to curtail the misappropriation of trade secrets would rely on one set of law in Maine (i.e., the Uniform Trade Secrets Act, which Maine has adopted), but an entirely different set of laws in Massachusetts (which is one of just two states that has not adopted Uniform Trade Secrets Act). Under that scheme, it is possible that the same misuse of company secrets would result in inconsistent outcomes depending on which state hears the case. Ideally, DTSA will provide more predictability to businesses bringing this claim, while still permitting companies to use those long-standing state remedies when preferable.

Holding Back High Praise

On the other hand, DTSA is in some ways less wave-making than it could have been. For starters, one could argue that the law does not improve the legal landscape in a substantive way. The federal government already had the power to enforce trade secret laws through criminal and civil actions, and state laws are mostly uniform and consistent in offering private remedies. In that sense, the immediate consequence of DTSA is to complicate and disrupt existing trade secret law. Trade secret litigation was already capable of being tedious and expensive, but with dual layers of state and federal law, cases are bound to become more complicated, as well as more costly.

Further, DTSA missed an opportunity to tailor protections for victims of cyber-hacking and cyber-espionage, a growing area of concern among some companies. Recent high-profile corporate hacks and espionage exploits have targeted Sony Pictures, DuPont, and Lockheed Martin, but smaller companies (often with comparatively less cyber-security) are also vulnerable to these types of attacks. A cynic might suggest that DTSA is merely the result of a dysfunctional Congress coming together to needlessly federalize legal protections already covered in near-uniformity by the states.

What Business Owners Need to Know Today

The main reason DTSA is generating some buzz is not because of what the law says, but rather the fact that it is going to affect many businesses. Exactly how it will affect businesses is less clear. Like with any new law, opinion is divided as to how DTSA's provisions will operate in the real world. For example, the *ex parte* civil seizure provision has the potential to offer swift and decisive justice to a victim of trade secret misappropriation, but it can also become a controversial weapon for bad faith actors who seek to unsettle their competitors.

Hopefully, most businesses will not need to discover first-hand how the federal law plays out in practice. But two things are certain: first, DTSA will usher more claims into federal courts, either as a standalone claim or as related breach of contract or unfair competition claims (which are state law matters) make it to federal court via supplemental jurisdiction when attached to a federal law claim. Second, DTSA reaches almost every business, from your brother-in-law's general contracting company to your uncle's accounting firm. Arguably every business has methods, data, or information that might be considered trade secrets, and every business with trade secrets can be economically harmed if that information is stolen or misused. Business owners must therefore act in advance if they hope to take full advantage of the law.

On that note, DTSA protects employees who disclose trade secrets in response to a court order or government investigation. In order to be eligible for all of the remedies created by DTSA, employers must provide notice of the statute's whistleblower immunity in any "contract or agreement with an employee that governs the use of a trade secret or other confidential information." That means confidentiality, non-disclosure, and non-compete agreements must be updated accordingly. Failure to do so may mean that a successful plaintiff cannot recover exemplary

damages or attorneys' fees as otherwise allowed by the statute.

Any business that may be affected by DTSA should also take this time to update policy manuals to include the appropriate immunity language. Form employment agreements used with employees who handle confidential business information will need to be modified. While agreements executed prior to May 12, 2016 are not required to have the whistleblower notice language, any businesses that entered into an employment agreement after May 12, 2016 will need to go back and amend those agreements to enjoy the full protection of DTSA. After all, if a company finds itself in the unfortunate situation of needing to use DTSA, it probably wants to have all of those brand new federal remedies at its disposal.

Trading Privacy For Safety: Where is the Line?

By Christopher C. Taintor, Esq.

1. **Medical Privacy: A Balance of Competing Interests**

In today's world, privacy and safety, two values important to all of us, are increasingly in tension. One need only read the news to see examples, the most recent of which is the battle between the Federal Government and Apple over access to a terrorist's cell phone. We all want the government to protect us from random violence. At the same time, though, we are reluctant to let the government know our secrets.

This tension is reflected in the laws that govern the confidentiality of medical information. Arguably, in fact, the tension is greatest there. On the one hand, it is important for anyone seeking out health care to feel confident in the privacy of the information they share with doctors, counselors, and other professionals. Medical privacy is fundamental, and not just because it give us comfort. Studies tell us that when patients don't feel assured of confidentiality, they don't tell their doctors everything they should, and the result of that reticence is that doctors are less able to provide quality care. On the other hand, though, the very fact that we share private information with our doctors means that the government sometimes views medical records as fertile sources of intelligence, a trove of information that can be used to prevent crime.

For better or worse, courts, and increasingly government agencies, have resolved this tension by imposing on health care providers a duty of disclosure that generally does not apply to others. Although there are exceptions to the rule, under Maine law an ordinary citizen who learns that an acquaintance poses a danger to another person, or to the public generally, typically has no duty to warn anyone of that danger. *Bryan R. v. Watchtower Bible and Tract Society of New York, Inc.,* 783 A.2d 839 (Me. 1999). There is a developing body of law, however, which imposes just such a duty on health care professionals. The result, ironically, is that the information people expect to be the most private is actually the most vulnerable to disclosure.

The seminal case pitting medical privacy against public safety is *Tarasoff v. Regents of University of California,* 551 P.2d 334 (Cal. 1976), where the California Supreme Court ruled that a psychotherapist may have a duty to warn third parties about a specific threat of harm to a foreseeable victim. In the forty years since *Tarasoff* was decided, nearly every state has adopted some variant of the rule, either by statute or by judicial decision.

2. The "Health or Safety" Exception to Maine's Medical Privacy Law

Although the Maine Supreme Judicial Court has never squarely addressed the issue, it has mentioned *Tarasoff* as a widely-recognized exception to the "no duty to protect" rule. Importantly, moreover, Maine's statute governing the confidentiality of health care records allows the disclosure of otherwise private information when a practitioner or facility "in good faith believes" that disclosure should be made "to avert a serious threat to health or safety." 22 M.R.S.A. §1711-C(6)(D). Although the Maine statute as originally enacted was quite vague, the Legislature recently added some clarity by amending it so that it now incorporates by reference the standards set out in the federal Privacy Rule (HIPAA). To satisfy that standard, the disclosure must be made in the good faith belief that it is "necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public," and it must be made "to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat." 45 C.F.R. §164.512(j).

Not surprisingly, health care practitioners feel some angst when they have to weigh patient privacy against public safety. Practitioners, especially therapists, ask with increasing frequency whether they have a duty to share information about patients who might be expected to harm others, and how that duty can be reconciled with their ethical obligations. In fact, though, the standards established in both Maine law and HIPAA actually give providers considerable discretion. In 2013, in the aftermath of the Newtown and Aurora tragedies, the Director of the Department of Health and Human Services Office of Civil Rights, which is responsible for enforcing HIPAA, took the remarkable step of sending an open letter addressed to "Our Nation's Health Care Providers," giving assurances that the law does not bar disclosure of otherwise confidential information "when necessary to . . . warn or report that persons may be at risk of harm because of a patient." Furthermore, he explained, "the provider is presumed to have had a good faith belief when his or her belief is based upon the provider's actual knowledge (i.e., based on the provider's own interaction with the patient) or in reliance on a credible representation by a person with apparent knowledge or authority (i.e., based on a credible report from a family member of the patient or other person). In short, a therapist or other professional is not obligated to accurately predict whether his or her patient is likely to harm someone. It is enough to have a "good faith belief" that disclosure is "necessary." Furthermore, as long as a clinician does not disclose private medical information with "malice," Maine law provides immunity from civil liability for malpractice or invasion of privacy.

From a risk management standpoint, the good faith standard and the qualified immunity defense combine to tip the legal scales in favor of disclosure. A therapist who thinks her patient *might* pose a "serious and imminent threat" to another, or to the public, may be better off reporting that concern than keeping it to herself. After all, if the therapist makes the report and the patient later sues for negligence or invasion of privacy, the clinician will have done what she could to avoid serious harm and will have a viable immunity defense. If, on the other hand, she is silent and the risk she feared materializes (i.e., the angry patient becomes violent and hurts someone), the adverse legal and professional may be much greater.

Violence, of course, is not the only risk that might be predicted based on information shared in a health care encounter. Doctors and other health care professionals may be put on notice of other risky behaviors – patients who continue to drive after they have become physically or mentally impaired, or who have unprotected sex after they have been diagnosed with sexually-transmittable diseases – and many wonder what they can and should say in those circumstances. If a doctor diagnoses a patient with a communicable disease and has good reason to think the patient will knowingly infect a partner, does he have an obligation to speak up? Around the country there are not only judicial decisions but state statutes imposing affirmative duties to disclose in these circumstances. See, e.g., Iowa Admin. Code §641-11.18(141A) (requiring physicians to notify their patients' known sexual or needle-sharing partners if they believe in good faith that patient, "despite strong encouragement," will not disclose HIV status); Mich. C.L.A. §333.5131 (same); Md. Code, Health – General §18-337 (same). Although Maine does not have a law requiring doctors to notify those whom their patients foreseeably might harm, it is conceivable that the dangers posed by these patients could be sufficiently "serious" and "imminent" to justify disclosure in at least some

circumstances (there are special confidentiality protections for patients who are diagnosed as HIV-positive). And if the doctor is at liberty to disclose, it is a short step to saying that he has an affirmative duty to reach out and protect his patient's partner.

3. Exceptions to the Exception

Not every health care professional practicing in Maine is regulated by Maine law and HIPAA. For some, the barriers to disclosure are higher.

Information acquired by an alcohol or drug abuse treatment facility, for example, has heightened protection under federal law. Alcohol and drug treatment facilities may communicate with law enforcement officers concerning "a patient's commission of a crime on the premises of the program or against program personnel or to a threat to commit such a crime."

42 C.F.R. 2.12(c)(5). Otherwise, disclosure of treatment records is permissible only pursuant to a court order, where "necessary in connection with investigation or prosecution of an extremely serious crime, such as one which directly threatens loss of life or serious bodily injury, including homicide, rape, kidnaping, armed robbery, assault with a deadly weapon, or child abuse and neglect." 42 C.F.R. 2.63. Under Maine law, the records of "Employee Assistance Programs" – programs created "to assist employees with family, legal, financial, mental health, and alcohol and other drug-related problems that may affect their ability to perform their jobs and their well-being" – are entitled to this same heightened degree of confidentiality. Code Me. R. tit. 14-118 Ch. 6, § V(C)(2)(a).

A different standard also applies to information acquired in the course of treating students. Under the Family Educational Rights and Privacy Act (FERPA), student health and counseling records can be disclosed only in a "health or safety emergency," where necessary "to protect the health or safety of the student or other individuals." The disclosure can be made to law enforcement personnel, public health officials, and trained medical personnel. 34 C.F.R. §99.31(a)(10) & §99.36

4. Conclusion

There is plenty of room for debate around the issue of medical privacy. Physicians believe that when patients lose confidence that their personal information will be kept private, that loss of trust undercuts the physician-patient relationship, which "could lead to negative, and possibly expensive, health consequences in other areas." Molnar & Eby, Medical Fitness To Drive & A Voluntary Reporting Law at 29-30 (AAA Foundation for Traffic Safety 2008). And in a variety of contexts, it has been found that being assured of confidentiality makes people more willing to seek medical treatment. Ford CA, et al. Influence of Physician Confidentiality Assurances on Adolescents' Willingness to Disclose Information and Seek Future Health Care: A Randomized Controlled Trial. *JAMA.* 1997; 278(12):1029-1034 (finding that adolescents are more willing to communicate with and seek health care from physicians who assure confidentiality). Gradually but surely, however, those assurances of confidentiality have been giving way to society's desire for protection. As we become ever more attuned to the risks around us, both patients and health care professionals would do well to be conscious of the shrinking scope of medical privacy.

NORMAN HANSON DETROY

Portland Office: (207) 774-7000
Lewiston Office: (207) 777-5200

Experienced. Efficient. Effective.

US-EU Announce Deal on Data Sharing "Privacy Shield" to Replace "Safe Harbor"

By Adrian P. Kendall, Esq.

Three months after the European Court of Justice struck down the US-EU "Safe Harbor" agreement in the case *Maximilian Schrems v Data Protection Commissioner* (C-362- 14), the EU and the USA announced in early February that they have agreed to a successor data protection regime. In the words of the European Commission: "This new framework will protect the fundamental rights of Europeans where their data is transferred to the United States and ensure legal certainty for businesses." The new EU-US "Privacy Shield" will again allow companies to store Europeans' personal data on American computers, subject to adherence to more rigorous compliance requirements.

Background:

The European Court of Justice had invalidated the "Safe Harbor" regime in the *Schrems* case by finding that it gave personal data of EU citizens insufficient protection against American intelligence gathering activities. Although the negotiations were at times rocky and hard fought, the stakes were too high for the parties not to find common ground: failure to reach a deal could have (i) led to economically and politically damaging enforcement litigation by EU nation state data protection agencies to prevent the transmission of personal data outside of the EU, and (ii) severely hampered the efficiency and effectiveness of multinational commercial activities.

"Privacy Shield" Summary:

The new arrangement will impose increased obligations on companies in the U.S. to protect the personal data of Europeans and requires stronger monitoring and enforcement by the U.S. Department of Commerce and Federal Trade Commission, including through increased cooperation with European Data Protection Authorities (DPAs). "Privacy Shield" includes commitments by the U.S. that access by public authorities to personal data transferred under the new arrangement will be subject to clear conditions, limitations and oversight, designed to prevent generalized access. Europeans will be able to raise any inquiry or complaint in this context with a dedicated new ombudsperson.

"Privacy Shield" Key Elements:

Business and industry representatives on both sides of the Atlantic have been asking for a clear and uniform interpretation of the *Schrems* ruling, as well as more clarity on the mechanisms they would be permitted to use to transfer data. The following elements of the "Privacy Shield" arrangement should provide a framework to address those concerns:

- **Strong obligations on companies handling Europeans' personal data and robust enforcement:** U.S. companies wishing to import personal data from Europe will need to commit to robust obligations on how personal data is processed and individual rights are guaranteed. The Department of Commerce will monitor that companies publish their commitments, which makes them enforceable under U.S. law by the Federal Trade Commission. In addition, any company handling human resources data from Europe has to commit to comply with decisions by European DPAs.
- **Clear safeguards and transparency obligations on U.S. government access:** For the first time, the US has given the EU written assurances that the access of public authorities for law enforcement and national security will be subject to clear limitations, safeguards and oversight mechanisms. These exceptions must be

used only to the extent necessary and proportionate. The U.S. has ruled out indiscriminate mass surveillance on the personal data transferred to the US under the new arrangement. To regularly monitor the functioning of the arrangement there will be an annual joint review, which will also include the issue of national security access. The European Commission and the Department of Commerce will conduct the review and invite national intelligence experts from the U.S. and European Data Protection Authorities to participate.

- **Effective protection of EU citizens' rights with several redress possibilities:** Any citizen who considers that their data has been misused under the new arrangement will have several redress possibilities. Companies will have deadlines to reply to complaints. European DPAs can refer complaints to the Department of Commerce and the Federal Trade Commission. In addition, alternative dispute resolution will be available free of charge. For complaints on possible access by national intelligence authorities, a new ombudsperson position will be created.

Next Steps:

This agreement marks a political resolution; the full, intricate legal framework has yet to be hammered out, so affected companies should still be adhering to the interim guidance. The EU College of Commissioners has mandated that Vice-President Ansip and Commissioner Jourová prepare a draft "adequacy decision" in the coming weeks. In the meantime, the U.S. side will make the necessary preparations to put in place the new framework, monitoring mechanisms and a new ombudsperson. Once the full framework is in place, affected US companies will need to gauge how they can effectively comply and at what cost as rigorous enforcement should be expected.

Time will tell if the goals of data security, trust and economic certainty will be fully met, especially on the issue of limited access by the NSA and other intelligence gathering agencies. Opponents have already voiced concerns over how any US safeguard assurances can be believed in the wake of the Snowden revelations and other spying activities that have recently become public. Another legal challenge may well loom, but it is highly likely that the European Court of Justice will uphold the "Privacy Shield" data protection scheme in the absence of specific proof of a breach.

Heavy Metal Lessons: Adventures in IP and Rock and Roll

By Adrian Kendall, Esq.

What can a lawyer learn from Heavy Metal band Metallica? When it comes to intellectual property protection and client relations, the answer is plenty.

On December 30, 2015, an IP lawyer sent a cease and desist letter to the members of Sandman, a Canadian Metallica tribute band, demanding that the band cease using the Metallica name and logo. Our clients work hard to develop value in their brands, so in the legal profession we use these letters all the time – that's standard procedure to stop unauthorized use ("infringement") and protect a client's valuable IP.

But Sheppard Mullin lawyer Jill Pietrini almost certainly did not count on her letter going viral and drawing the ire of the band's fans. Per Metallica's very public apology in Rolling Stone, the attorney apparently did not consult with her clients before sending the letter. Calling their own lawyer "very overzealous", Metallica told Sandman they could "file the letter in the trash" and to "keep doing what you're doing … we totally support you!"

As for their lawyer, the legendary rockers said: she "can be found at SFO catching a flight to go permanently ice fishing in Alaska." Hopefully that was an overstatement and the attorney and client have since worked together to reset expectations, but there are a couple of clear lessons for lawyer-client relationships:

- Lawyers should always consult with clients on action taken to protect their interests, especially where it can affect a very public brand, and they should work together to establish clear standards for anti-infringement action if it's going to be "automatic". Digital media is a double edged sword: it can be a powerful agent for change and promotion, but it can also make backlash virtually instantaneous and global.
- When suggesting a course of action to protect a client's IP, lawyers and their clients should consider every aspect of how the infringing party is using the mark. Not every technical infringement needs to be shut down. In this case, the tribute band probably enhances the Metallica brand. If any action was necessary at all, a letter to the tribute band acknowledging the use and offering a revocable and limited, non-transferable license might have been the better approach.

Rock on!

Maine Legislature Approves Significant Increase in Maine Estate Tax Exemption Level

By Kathryn M. Longley-Leahy, Esq.

Effective January 1, 2016, the Maine estate tax exemption will more than double from its current $2,000,000 level to the applicable federal estate tax exemption, currently $5,430,000, indexed annually for inflation. With this significant increase in the Maine estate tax exemption, Maine estate tax exposure will be effectively eliminated for each Maine resident and non-resident owning property in Maine whose available estate tax exemption as of the date of death, is less than $5,430,000, as indexed.

While Maine's new estate tax legislation falls short of including the additional benefit available under federal estate tax law that allows a surviving spouse to add to his/her available estate tax exemption the 'unused' exemption of the first deceased spouse1), and continues to bring back into the Maine taxable estate the value of reportable gifts made within one (1) year of the Maine decedent's date of death, ***Maine's new estate tax legislation raises the Maine estate tax exemption to historic levels, thereby eliminating Maine estate taxation for the vast majority of Maine taxpayers***.

Given the multitude of fluctuations in federal and Maine estate tax laws over the last few decades, many estate plans, particularly those for married couples, have already incorporated planning mechanisms to absorb potential changes in federal and state estate tax laws by creating certain trusts, funded directly or indirectly via disclaimer provisions, to ensure that estate tax exemption available to each individual is fully utilized; however, if the trusts were created solely to minimize estate taxes, such "exemption" trusts may no longer be necessary. Following any life or legislative change, one needs to be diligent in confirming that existing estate planning documents continue to reflect current estate planning objectives. The estate planning group at Norman, Hanson & DeTroy is always available to provide assistance should you have any questions, concerns or simply want to confirm that your current estate planning documents continue to reflect your current planning objectives.

NORMAN HANSON DETROY

Portland Office: (207) 774-7000
Lewiston Office: (207) 777-5200

Experienced. Efficient. Effective.

Notable Changes to Maine Employment Laws

By Kelly M. Hoffman

In its recently concluded session the Maine Legislature enacted L.D. 921 "An Act To Strengthen the Right of a Victim of Sexual Assault or Domestic Violence To Take Necessary Leave from Employment and To Promote Employee Social Media Privacy." The new bill imposes two significant changes to employment laws that affect all Maine employers of any size and will become effective on October 14, 2015.

1.Employment Leave For Victims of Violence

The first part of the law increases penalties for employers that fail to grant reasonable and necessary leave from work to employees who are victims of domestic violence, sexual assault, stalking, and other acts that would support a court order for protection. 26 M.R.S. § 850. If the Maine Department of Labor ("DOL") receives notice of a violation of the law within six (6) months of the occurrence, the DOL **may** fine noncompliant employers up to $1,000.00 per occurrence. The previous law provided that the DOL could only fine employers no more than $200.00 per occurrence. In addition to fines that may be paid to the DOL, the law further dictates that the employer **must** pay liquidated damages to the employee in an amount equal to three (3) times the amount of total assessed DOL fines.

If the employee is unlawfully terminated, she may choose one of two remedies: either the employee may elect the treble damages discussed above or she can demand re-employment with back wages.

In addition to protections provided by this law, an employee also may be entitled to protected leave under the Maine Family Medical Leave Requirements Law or the federal Family Medical Leave Act if she has sustained a qualifying medical condition as a result of domestic violence or is needed to care for certain family members with such conditions.

An employee who has suffered a serious physical or mental injury as a result of domestic violence also may be disabled for purposes of the Americans with Disabilities Act ("ADA") or the Maine Human Rights Act ("MHRA"). Both laws require employers to provide reasonable accommodations to employees with disabilities. For example, an employer who has an employee with a traumatic brain injury caused by a domestic violence assault would likely be required to provide her with a reasonable accommodation, such as a modified work schedule so that she may attend speech or occupational therapy. The ADA and MHRA also may require an employer to provide an employee with a protected period of leave from work as a reasonable accommodation for a disability even if the employer is not subject to Maine or federal medical leave laws.

The prohibitions against sexual or sex-based harassment in the MHRA and Title VII of the Civil Rights Act of 1964 further may be applicable to situations involving domestic violence arising from workplace relationships. Such harassment may create a hostile work environment in violation of the MHRA or Title VII if it is so severe or pervasive that it alters the employee's terms and conditions of employment. For example, a violation of either law may exist if an employer does not take prompt and sufficient action after an employee makes her employer aware that her ex-boyfriend, a coworker, has emailed sexually suggestive photos of her to other employees and has repeatedly subjected her to derogatory sexual comments.

2.Employee Social Media Privacy

The second part of the Act addresses social media accounts. This portion of the Act will be codified at 26 M.R.S. §§ 615-619. These laws will have widespread day-to-day application because an employer's ability to demand or even request access to an employee's or applicant's social media accounts is restricted. Social media accounts are defined broadly to include e-mail, videos, blogs, texts, text messages, podcasts, and websites. An employer cannot demand or request passwords or other access to any social media accounts and cannot make employment decisions based on an employee's or applicant's refusal to provide such access. An employer likewise cannot require an employee or applicant to alter her settings so that a third-party is able to view the contents of a personal social media account. An employer further cannot require an employee or applicant to "friend" anyone (including the employer or its agent).

However, the law does not limit the employer's ability to establish and enforce lawful workplace policies addressing the use of the employer's electronic equipment, including a requirement that employees disclose their user name, password, or other information to access the employer-issued electronic devices, such as cell phones and computers, or to access employer-provided software or e-mail accounts.

The law does provide a few exceptions. Employers are allowed to require that employees disclose personal social media account information that employers reasonably believe to be relevant to an investigation of allegations of employee misconduct or a workplace-related violation of applicable laws, rules, or regulations. This provision applies only when not otherwise prohibited by law, as long as the information disclosed is accessed and used solely to the extent necessary for purposes of that investigation or a related proceeding.

As to banking and securities laws, another exception provides that employers may comply with a duty to screen employees or applicants before hiring or to monitor or retain employee communications that is established by a self-regulatory organization as defined by the federal Securities Exchange Act of 1934. This exception applies to the extent necessary to supervise communications of regulated financial institutions of insurance or securities licensees for banking-related, insurance-related or securities-related business purposes.

An employer who violates these new statutory provisions is subject to a fine imposed by the Department of Labor of not less than $100.00 for the first violation, not less than $250.00 for the second violation, and not less than $500.00 for each subsequent violation.

All employers should review their personnel policies to ensure consistency with this new law and may contact employment counsel, including those at Norman, Hanson & DeTroy, for further guidance with these matters.

Maine's Anti-SLAPP Statute: A Tool for Litigators

By: J.D. Hadiaris

Defending a claim for defamation, libel, or abusive litigation (i.e., malicious prosecution or abuse of process) can be difficult and time consuming. Even when the plaintiff's claim is weak and the damages small, these cases often require substantial discovery practice before a motion for summary judgment can be filed. Factual disputes can preclude summary judgment, and defendants or their insurers may have to consider paying money to settle a case simply to avoid further litigation costs. Given the practical difficulties of defending these claims, it is important to

consider Maine's anti-SLAPP statute, 14 M.R.S.A. § 556, when answering a lawsuit that arguably involves the right to "petition."

SLAPP is an acronym for Strategic Lawsuit Against Public Participation. SLAPP litigation, generally, is litigation without merit filed to dissuade or punish the exercise of First Amendment rights of defendants. *Morse Bros. v. Webster, 2001 ME 70, ¶ 10, 772 A.2d 842, 846*. Maine's anti-SLAPP statute is designed to guard against meritless lawsuits brought with the intention of chilling or deterring the free exercise of a defendant's First Amendment right to petition the government by threatening would-be activists with litigation costs. *Schelling v. Lindell*, 2008 ME 59, ¶ 6, 942 A.2d 1226, 1229. In furtherance of this purpose, the anti-SLAPP statute allows a defendant to file a special motion to dismiss claims against it that are based upon the defendant's exercise of the constitutional right to petition. *Nader v. Maine Democratic Party*, 2013 ME 51, ¶ 12, 66 A.3d 571, 575.

The Maine Law Court has repeatedly recognized that Maine's anti-SLAPP statute "very broadly defines the exercise of the 'right to petition.'" *Schelling*, 2008 ME 59, ¶ 11, 942 A.2d at 1230; *see also Nader v. Maine Democratic Party*, 2012 ME 57, ¶ 28, 41 A.3d 551, 560. The Law Court has stressed that it "is clear from the language of section 556 [that] the Legislature intended to define in very broad terms those statements that are covered by the statute." *Schelling*, 2008 ME 59, ¶ 12, 942 A.2d at 1230; *see also Maine's Anti–SLAPP Law: Special Protection Against Improper Lawsuits Targeting Free Speech and Petitioning,* 23 Me. Bar J. 32, 37 (2008) at 35 (Maine's anti-SLAPP statute "manifests a breadth of scope beyond that of many other states' anti-SLAPP laws"). Section 556's broad definition of the right of petition includes the following:

1. Any written or oral statement made before or submitted to a legislative, executive or judicial body, or any other governmental proceeding;
2. Any written or oral statement made in connection with an issue under consideration or review by a legislative, executive or judicial body, or any other governmental proceeding;
3. Any statement reasonably likely to encourage consideration or review of an issue by a legislative, executive or judicial body, or any other governmental proceeding;
4. Any statement reasonably likely to enlist public participation in an effort to effect such consideration, or any other statement falling within constitutional protection of the right to petition government.

14 M.R.S.A § 556. The statute does not limit the definition of petitioning activity to statements made to a governmental body or representative. *Id.*; *see also Maine's Anti–SLAPP Law: Special Protection Against Improper Lawsuits Targeting Free Speech and Petitioning,* 23 Me. Bar J. 32, 37 (2008) at 35 ("Section 556 is by its explicit terms, quite broad, providing its qualified immunity to even the most indirect of exercises of one's right to petition the government"). In *Maietta Construction, Inc. v. Wainwright*, the Law Court held that letters written to the city council, to the mayor, as well as statements made to the newspapers "clearly amount to petitioning activity" for the purposes of the anti-SLAPP statute. 2004 ME 53, ¶7, 847 A.2d 1169. Likewise, in *Schelling,* the Law Court held that a letter to the editor, arguably intended to effect reconsideration of an issue by the Legislature, was within the definition of petitioning activity. 2008 ME 59, ¶13, 942 A.2d 1226, 1230-1231. Other courts have also held that pleadings filed in court constitute "petitioning" activity, because they are "statement[s] reasonably likely to encourage consideration or review of an issue by a … judicial body."

The anti-SLAPP statute provides that a special motion to dismiss "may" be filed within 60 days after the date of service of the complaint, or at any time later at the discretion of the court. Given the 60-day window, it is important to consider whether the statute may apply at the time of the answering of the complaint, or soon thereafter. The 60 day period will expire before the deadline to amend pleadings under the court's Standard Scheduling Order, and courts in Maine have in some cases been unwilling to extend that deadline beyond the 60-day period.

The primary benefit of the anti-SLAPP statute, from the defendant's perspective, is that it gives the defendant the

ability to move to dismiss the claim at the outset, before the defense incurs significant costs. It also allows the defendant to move to dismiss a claim where the plaintiff's complaint is not based upon "actual damages." This is important because in defamation or libel cases, a plaintiff is generally allowed to pursue a claim based upon "per se" damages if the alleged defamatory statements are related to the plaintiff's work, allegations of criminal activity, or "scandalous diseases." In other words, a defendant may pursue a claim for nominal damages, even where he has not suffered any actual harm.

When filing a special motion to dismiss under the anti-SLAPP statute, the defendant has the initial burden of demonstrating that the anti-SLAPP statute applies by showing that the claims are based on the defendant's conduct in exercising his/her constitutional right to petition. If the moving party establishes that the anti-SLAPP statute applies, the burden shifts to the non-moving party, and under the second step, the court *must* dismiss the action unless the non-moving party makes a *prima facie* showing, through pleadings and affidavits, that at least one of the moving party's petitioning activities "was devoid of any reasonable factual support or any arguable basis in law … and caused actual injury to the [non-moving] party." *Town of Madawaska v. Cayer*, 2014 ME 121, ¶ 9, 103 A.3d 547, 550; (*citing Nader*, 2013 ME 51, ¶ 14, 66 A.3d 571). This can often be a difficult burden for the plaintiff to prove, and one that the plaintiff would not need to meet if the case were to go to trial.

If a party succeeds on his or her special motion to dismiss, the court has discretion to award attorney's fees to the defendant.

The other benefit is that the special motion to dismiss under the anti-SLAPP statute is generally decided based upon a limited factual record. The defendant will generally move to dismiss based upon the allegations of the complaint, and may attach affidavits if necessary. The plaintiff will then respond by submitting affidavits as well. The court will make a decision on the motion to dismiss by considering this limited record.

Additionally, unlike the denial of a summary judgment motion, the denial of a special motion to dismiss is immediately appealable. Therefore, if the defendant loses a special motion to dismiss, he or she can appeal the decision to the Law Court before expending any further significant funds on discovery (discovery is stayed upon the filing of a special motion to dismiss). The appeal from a denial of a special motion to dismiss is generally reviewed *de novo*, meaning the trial court's ruling is not given any weight on appeal.

Based upon these potential benefits, it is important consider the anti-SLAPP statute's special motion to dismiss whenever a complaint for defamation or abusive litigation is filed. Doing so may protect defendants and their insurers from costly litigation, and from having to consider "nuisance" settlements.

Health Record Audit Trails: How Useful is the Metadata that is Associated with a Patient's Health Record?

By Jennifer A.W. Rush, Esq.

Gone are the days when your doctor carried a manila folder into the exam room with her, shuffling through it to find the last office visit note or your current list of medications. Paper charts have been replaced by electronic health records, or "EHRs," which are now in wide use in hospitals and medical practices around the country. Now, doctors carry their laptops everywhere with them, retrieving and creating health information with a click of a button.

We are slowly catching up with what this technology has to offer, and the problems it creates, when it is used in litigation. By now, we have all heard about electronic discovery. In fact, almost every time we request a medical record, we are engaging in a form of electronic discovery because the "record" can no longer be photocopied from a chart on a shelf, but must be transferred from an electronic format into a format that is compatible with production. Not being able to inspect the original paper chart at a deposition and instead trying to determine if everything has been printed from the computer is a task to which all those who litigate injury claims have become accustomed. We are also mindful of the fact that what the physician or nurse sees on the screen when viewing a patient's record looks markedly different from the format in which it is printed. Moreover, information in the EHR changes over time in ways that information in a paper chart cannot. Added to these changes is the fact that with EHRs, there is "information about the information" – metadata about the record that never existed with paper charts and is kept in an "audit trail." We are beginning to see routine requests for the "audit trail" associated with the EHR, and the benefits and problems that these requests bring to litigation are just beginning to surface.

A.What is an "audit trail"?

An audit trail can be defined in basic terms as a "record that shows who has accessed a computer system, when it was accessed, and what operations were performed." Brodnik, Melanie, et al., *Fundamentals of Law for Health Informatics and Information Management*. Chicago, IL: AHIMA, 2009, 215. Pursuant to the Health Insurance Portability and Accountability Act (HIPAA), medical providers who use EHRs must have systems in place to review and audit access to records, as well as prevent unauthorized access. 45 C.F.R. §§ 164.308(a)(1)(ii)(D), (a)(3)(i), 164.312(1)(b). Compliance with HIPAAs requirements is routinely obtained through the use of audit trails, which track the information required by HIPAA and provide a mechanism for determining if there has been a security breach.

One of the problems is that there are a variety of different vendors of EHRs and thus, a variety of different formats for audit trails. If you are using audit trails in litigation, you cannot count on the audit trail from Hospital X to look anything like, or contain the information contained within, the audit trail from Hospital Y. EHR certification requirements mandate that the following data be recorded in an audit trail: type of action (additions, deletions, changes, queries, print, copy); date and time of event; patient identification; user identification; and identification of the patient data that is accessed. *Health Information Technology: Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology*, 2014 Edition; Revisions to the Permanent Certification Program for Health Information Technology, Final Rule (September 4, 2012). Beyond these basic requirements, there is a wide variety of information recorded among different EHR vendors.

B.How are audit trails used in litigation?

Audit trails are not part of the "patient record" and should not be automatically produced when there is a request for the record. Instead, they must be specifically requested and the validity of the request must be analyzed on a case-by-case basis. The request for an audit trail, like any other discovery request, is subject to Maine Rule of Civil Procedure 26's requirement that the request be "reasonably calculated to lead to the discovery of admissible evidence."

As everyone involved in litigation knows, Rule 26's standard is a broad one. Nonetheless, there is a duty on the part of the individual making the request to at least articulate why the audit trail might provide admissible evidence in the case.

By far, the most common use of audit trails is in medical malpractice actions. For example, if there is a question of when a physician viewed an x-ray report, or a lab result, the audit trail may be able to provide that information. This may have a significant impact on the liability of the medical provider. If the timing of a particular chart entry is

important to the prosecution or defense of a case, then the audit trail may be able to shed light on that issue. In any personal injury case where the plaintiff's compliance may be an issue, audit trails may be able to reveal information regarding how many times the patient changed or failed to show for his appointment, for example. Moreover, if the plaintiff's presentation at a specific office visit is important and the chart does not identify the nurse who admitted the patient, then the audit trail should contain that information and lead to the identity of a potentially key witness.

C.Audit trails cannot be used in a vacuum; they require explanation.

In general, audit trails make poor witnesses and are simply launching pads for additional discovery. They are indecipherable to most people, inconsistent between medical practices, and often unreliable. When justifying their request for an audit trail, requesting parties often argue that the trail will tell them exactly what information was accessed and modified by what user, and when, but in reality the story told by an audit trail is rarely that straightforward. The audit trail seldom reveals the substance of the information that was changed or added. We also know that even though they are supposed to do so, system users often fail to "log off." For example, if a physician and a nurse happen to be in the emergency department exam room at the same time, they may both enter information into the computer but will use only one person's log-in information.

A case example involving Northshore University Health System provides an excellent example of why the use of audit trails should be approached with caution. In that particular case, the parties had already spent an extraordinary amount of time and resources on the production of the EHR and the plaintiff held a fair amount of suspicion regarding the accuracy, completeness, and reliability of the HER itself. Chris Dimick, *EHRs Prove a Difficult Witness in Court*, Journal AHIMA (Set. 24, 2010). When it came time to producing and dissecting the audit trail, even more suspicion arose, even though the explanations for the purported inconsistencies were explained by technology and completely outside of the hospital's control.

By way of background, when audit trails are printed, they look like Excel documents. One column will include the patient's identifier, which is usually a unique combination of letters and numbers assigned to that specific patient. Sometimes, however, an individual patient will have several different identifiers that are unique to the hospital admission or the type of care received. Radiology departments, for example, usually use their own electronic record systems that interface with the patient's other electronic records. Another column, or columns, will provide one or more date stamps, depending on the vendor of the EHR. Additional columns will identify the user of the record by name, a unique code, or both. The general description of the portion of the record accessed will be provided in another column, but the description is generally not specific enough to provide true substantive information. For instance, the description may be "VITALS GRAPHIC I&O REPORT," which will reveal that the user viewed the patient's record of volume input and output, but does not tell us what information on that I&O report was viewed. Or, the entry may simply read "NURSES NOTES PROGRESS NOTE REPORT," which tells us absolutely nothing about what progress note during a multi-day admission was viewed by the user at that particular time.

Another column in the audit trail will indicate the "action," which is where Northshore University Health Systems ran into problems. The "action" is usually described by one word – query, modify, accept, view, etc. As with most audit trails, Northshore's audit trail's use of the word "accept," meant different things depending on the type of record and the circumstances. It could mean that the record was pended, filed, shared, or actually accepted by a physician. Chris Dimick, *EHRs Prove a Difficult Witness in Court*, Journal AHIMA (Set. 24, 2010). This became a problem when the audit trail documented an "accepted" physician order that did not appear in the EHR. Northshore did not erase the order from the record or withhold it from production as one might infer, however. Instead, "accepted" in that particular instance meant that the order was "pended." Because the order was never executed, it never appeared in the EHR even though it appeared, from the audit trail, as though it was an "accepted," or final, order. *Id*.

There have been other cases were time stamps have proved unreliable. In one case, the audit trail produced by a

hospital showed that the user opened dozens of documents within the same second. The IT department demonstrated that it was physically impossible to open all of the documents at the same time, and likewise physically impossible to view them all at the same time. The best explanation provided by the IT department was that when one document was opened, the system showed all the documents in that "batch" or grouping as having been opened. The audit trail in that instance proved meaningless when trying to sort out whether a specific person actually viewed a specific document.

D.Practical implications in litigation.

Parties who request and use audit trails must be aware that although they may prove useful in some cases, they will, invariably, require explanation. At a basic level, the parties must become educated on what the information in the various columns means, and whether it is reliable. If the audit trail comes from a hospital, then the hospital may need to produce a member of its IT department for a deposition. Smaller medical practices, however, may not employ anyone who possesses enough knowledge about the audit trail to provide litigants with meaningful information. After all, the audit trail was not designed to be used in litigation. It is a compliance tool that enables medical providers who use EHRs to meet the requirements set forth by HIPAA. In these cases, parties may need to go to the source – the vendor of the EHR – or hire experts in order to give meaning to the information in the trail.

The added time and cost associated with this discovery is not warranted in every case. By the time the parties have concluded that the information in the audit trail justifies the added burden, however, the medical provider may have changed vendors for its EHR, archived the trail (which can make the data even more incomprehensible), or otherwise lost or destroyed the data that the parties seek. Accordingly, at least in medical malpractice actions where the health provider is a party, a well-crafted litigation hold letter in lieu of an automatic discovery request for the audit trail makes practical sense. Parties must also remember that audit trails contain protected health information. Accordingly, requests for audit trails that are maintained by non-parties must be accompanied by a Court order or a valid release that is signed by the patient. Moreover, litigants should not be surprised if health care providers require subpoenas in addition to patient releases before they will produce audit trails; the obligation on the part of a provider to produce the audit trail, as opposed to some other method of "accounting of disclosures" is not well-defined under HIPAA regulations.

In summary, we are just beginning to understand the potential uses and burdens that are associated with the metadata attached to EHRs. The request for this metadata is not subject to the Rules of Civil Procedure alone, but must be analyzed within the framework of HIPAA and IT considerations. One thing is for certain, the change from paper records to electronic health records means that litigants must change their practices in how they request, interpret, and use medical records. And, in cases where the audit trail is a relevant source of information, this change will mean added cost and burden to litigants.