HIPAA-Compliant Court Orders in Personal Injury Cases

Prepared by:
Robert D. Fink
Sofia Zneimer
Cynthia S. Kisser

There are growing concerns over privacy, collection, and use of personal data in the United States, Europe,[1] and elsewhere. Data scientists, privacy advocates, politicians, and citizens are sounding the alarm on data collection, use, and abuse. Companies harvest, consolidate, and weaponize seemingly random data bits like shopping patterns, social media posts, online connections, zip codes, driving patterns, housing, credit history, reading patterns, politics, and other personal details, and are looking for loopholes to combine regulated data with unregulated data from social media and use it in the lucrative opaque business of predictive analytics. Health data has enormous value to data brokers and to insurance companies in devising various predictive analytical tools. These analytical tools are not fine-tuned for fairness or objectivity. Instead, they often hide biases behind proxies (for example, use of a zip code in a poor neighborhood to disguise the bias that people in poorer areas may not shop for insurance, and therefore could be charged higher premiums), and increase the power mismatch between insurance companies and data subjects.

In July 2018, ProPublica (www.propublica.org) co-published an article with National Public Radio (www.npr.org), entitled *Health Insurers Are Vacuuming Up Details About You — And It Could Raise Your Rates,*[2] which raises concerns about the lack of public scrutiny over insurance companies teaming up with data brokers to collect data to determine coverage and rates:

> The companies are tracking your race, education level, TV habits, marital status, net worth. They're collecting what you post on social media, whether you're behind on your bills, what you order online. Then they feed this information into complicated computer algorithms that spit out predictions about how much your health care could cost them….Are you a woman who recently changed your name? You could be newly married and have a pricey pregnancy pending. Or maybe you're stressed and anxious from a recent divorce. That, too, the computer models predict, may run up your medical bills. Are you a woman who's purchased plus-size clothing? You're considered at risk of

depression. Mental health care can be expensive. Low-income and a minority? That means, the data brokers say, you are more likely to live in a dilapidated and dangerous neighborhood, increasing your health risks.

Data Scientist Cathy O'Neil raises the alarm that profit-tuned algorithms cause "feedback loops" (she calls them "Weapons of Math Destructions") that increase social ills. In the book *Weapons of math destruction: How big data increases inequality and threatens democracy*, [3] she argues that these "feedback loops" feed on each other:

> Poor people are more likely to have bad credit and live in high-crime neighborhoods, surrounded by other poor people. Once the dark universe of WMDs digests that data, it showers them with predatory ads for subprime loans or for-profit schools. It sends more police to arrest them, and when they're convicted it sentences them to longer terms. This data feeds into other WMDs, which score the same people as high risks or easy targets and proceed to block them from jobs, while jacking up their rates for mortgages, car loans, and every kind of insurance imaginable. This drives their credit rating down further, creating nothing less than a death spiral of modeling. Being poor in a world of WMDs is getting more and more dangerous and expensive. [4]

In the book O'Neil gives an example of how Allstate Insurance used algorithms studying proxies that have nothing to do with driving risk, to charge more:

> But consider the price optimization algorithm at Allstate, the insurer self-branded as "the Good Hands People." According to a watchdog group, the Consumer Federation of America, Allstate analyzes consumer and demographic data to determine the likelihood that customers will shop for lower prices. If they aren't likely to, it makes sense to charge them more. And that's just what Allstate does. [5]

As of the writing of this article, Cathy O'Neil's 2017 book has been cited by peer-reviewed publications 745 times on Google Scholar.[6]

Of all the data, the value of the information from medical records cannot be understated. Medical records have detailed information of a person's most intimate personal details, and such information has value for insurance companies and data brokers far beyond its use to settle the claim brought by the data subject. While the fact that a woman is shopping for a larger dress or buying clothes in the baby section of a store may or may not mean the shopper is pregnant, the medical records can take the guess out, and will confirm such correlation. In the future, a

woman shopping in an infant store section may end up with increased health insurance rate because the algorithm could predict she may be pregnant, whether or not she is, and she will have no idea that her shopping for a friend's baby shower caused her health insurance rates to spike. The insurance companies collect and retain medical records without the records' subject ability to any give input about the use or retention of medical records.

In today's age of Big Data and associated concerns over data breaches and how personal data is used, many people still do not know that their Personal Health Information (PHI) comes into play when they file a personal injury case-- or what happens to their PHI once it does. The privacy issues surrounding the use of PHI are supposed to be addressed using a qualified protective order (QPO). A QPO should be entered by a court in cases in which a party places his/her health at issue and is intended to allow for the limited disclosure and use of protected health information (PHI) during the pending litigation. In 1996, the Health Insurance Portability and Accountability Act, or HIPAA, became federal law. Although intended to protect the privacy of a patient's medical records, an unintended consequence of the Act has been to create confusion in the courts as to the implications for disclosure of the health care information HIPAA is intended to protect where a plaintiff has placed his or her health care at issue in a personal injury claim.

Perhaps nowhere is this confusion more evident in Illinois than in the attempts of the Law Division of the Circuit Court of Cook County to craft a HIPAA Protective Order that allows the defendant access to a plaintiff's protected healthcare information (PHI) for use during the litigation, while mindful of the fact that both constitutional and statutory rights control the conditions under which PHI can be produced in litigation. A review of the development of the Cook County HIPAA Protective Order, which became effective in October 29, 2018, and which requires both a plaintiff and his/her counsel to sign the Order,[7] illustrates both the issues contributing to this confusion, and offers insight into the need for a uniform HIPAA Protective Order for personal injury cases throughout the Illinois court system, and the problems that must be addressed for such an Order to respect the plaintiff's constitutional and statutory rights.

History of the HIPAA Protective Order in the Circuit Court of Cook County, Law Division.

The HIPAA Order, required by General Administrative Order 18-1 (G.O. 18-1) of the presiding judge of the Law Division of the Circuit Court of Cook County[8] traces its genesis to

efforts by the trial court in the matter of *Shull v. Ellis* (Cook County case 15 L 975) and all consolidated cases, in which State Farm Mutual Automobile Insurance Company, not the plaintiff, intervened and took issue with the language of the standard Law Division HIPAA order then in use in that Division since 2012.[9]

The 8-paragraph 2012 Order limited access to a plaintiff's PHI to the current parties and future parties to the litigation, and to their attorneys and certain persons associated with those attorneys firms. It allowed covered entities, as defined by 45 C.F.R. 160.13, to disclose PHI reasonably connected to the litigation; required its return or destruction at the end of the litigation, and did not relieve any party from compliance with the certain federal and state laws pertaining to mental health, drug and alcohol treatment and other records that enjoy heightened protections.

State Farm argued that the 2012 Order, which required the return or destruction of the PHI, conflicted with an insurer's federal and state statutory obligation to preserve the PHI for seven years pursuant to 215 Ill. Com. Stat. Ann. 5/133, [10] and that this mandatory retention also permitted insurers to use a plaintiff's PHI in the future, without limitation, including for use against a plaintiff in future litigation or for business purposes not related in any way to litigation in which the plaintiff brought the claim.

The *Schull* court accepted State Farm's position that the Illinois Insurance Code ("IIC), along with its regulations, requires this retention of PHI received in litigation for seven years, and identified three areas where the QPO then in use by the Law Division conflicted with federal and state law and the Illinois constitution:

1) the disclosure of a plaintiff's PHI to property and casualty insurers, although HIPAA allows no such disclosure in litigation;

2) the disclosure of a plaintiff's PHI to property and casualty insurers without the plaintiff's explicit and knowing waiver of her constitutional right to privacy, and

3) the restriction that property and casualty insurers retain PHI only until the end of litigation, although the *Shull* court believed the IIC required them to retain PHI for at least seven years.[11]

To resolve this conflict, the *Shull* court crafted a new HIPAA Order, which was entered July 25, 2017 as General Order 17-3, that required the plaintiff to sign a waiver of his/her constitutional right to privacy as to all PHI so that "the waiver will assure that property and

casualty insurers may use what would otherwise be considered PHI as mandated by state law."[12] It expressly listed ten uses allowed under the Order, only some of which were litigation-related.[13] G.O. 17-3 was stayed pending further order of the Court. General Order 17.4 was entered December 15, 2017 which officially vacated G.O 12-1 and 17-3.[14]

G.O. 17-4 incorporated a waiver of plaintiff's constitutional right to privacy as to all PHI, and requiring that the plaintiff understood that by refusing to consent to the contents of the order, the court may impose sanctions up to and including dismissal of the complaint.[15] G.O 17-4 authorized non-litigation as well as litigation uses of PHI by insurance companies, and identified eleven expressly identified uses permitted by insurance companies.[16]

G.O 17-4 generated multiple objections from the plaintiff's bar; including that it included language that violates both a plaintiff's constitutional and statutory rights as the price of litigating in Cook County. In addition, paragraph 6 of the Order prohibited any party from requesting, obtaining, or disclosing PHI, which effectively precluded the plaintiff and the plaintiff's attorney to receive or use PHI.

In response to the objections, the General Order was amended again, on October 29, 2018. General Order 18-1 (G.O. 18-1) was modified expressly stating that the Order does not relieve stakeholders from compliance with a list of Illinois and Federal privacy laws. [17] It also changed paragraph 6 to "Other than the party who disclosed PHI or that party's attorneys" as stakeholders that need a court order to receive PHI.[18]

G.O. 18-1 also required the plaintiff to sign a waiver of his/her constitutional right to privacy as to all PHI in favor of insurance companies, leaving in place the eleven uses allowed under the previous General Orders, including uses that were not litigation-related.[19] Neither the *Schull* Court nor any of the recent General Orders address the issue of why any insurance company is entitled to receive any PHI at all-- as they are not an entity authorized by HIPAA to receive PHI.

This article discusses the conflicts with federal and state law and the Illinois Constitution inherent in 2018 Cook County G.O. 18-1, and identifies the requirements necessary to make any such order both HIPAA-compliant and constitutionally sound.

A HIPAA Order cannot force a Plaintiff to waive Constitutional rights as a condition of litigating in Illinois.

The Illinois Constitution guarantees all citizens a right to access its courts to seek justice.[20] It also guarantees its citizens a right to privacy.[21] Further, the U.S. Constitution protects a citizen's right to privacy.[22] Under the language of General Order 18-1, the most recent Cook County Law Davison's HIPAA Order (the October 29, 2018 Order), a plaintiff is required to waive his/her rights to privacy to *all* PHI as a condition of accessing the courts to bring a personal injury claim. This Order violates a plaintiff's rights under the Illinois constitution, and exceeds the authority allowed a court pursuant to HIPAA in regard to disclosure of PHI in litigation.

HIPAA recognizes that patients bring legal claims that involve the disclosure of medical information. For this reason, it permits disclosure of PHI for use in judicial and administrative proceedings by order of a court.[23] However, the disclosure must be limited to "only the protected health information expressly authorized by such order"[24] The disclosed information must be used for no other purpose than the litigation, and the PHI must be returned or destroyed at the termination of the litigation.[25]

The G.O. 18-1 HIPAA Order does not delineate the PHI that it authorizes release of, thereby requiring plaintiffs who bring personal injury claims to waive their right to privacy, not just as to PHI related to the injury at issue, but also as to unrelated PHI as well. G.O. 18-1 requires a near blanket waiver as to all PHI rather than to expressly relevant PHI—i.e., injuries close in time and related to the same part of the body upon which the personal injury claim rests, to which the plaintiff must agree or face sanctions.[26] G.O. 18-1 also specifically exempts insurance companies from complying with the HIPAA regulation, which mandates return or destruction of the PHI upon conclusion of the litigation. 45 C.F.R. §164.512(e). [27]

The Illinois Supreme Court long ago held that the constitutional protection against unreasonable searches and seizures means that while a court may compel the production of records upon a proper showing that they contain entries tending to prove the issues, no right is given to compel the submission of records for general inspection and examination, for fishing purposes, or with the view of finding evidence to be used in other suits or prosecutions; it cannot be used for general investigation of a transaction not material to the issue.[28] These principles were applied to the privacy interest in medical information in *Kunkel v. Walton.*[29] In *Kunkel*, the Illinois Supreme Court considered the constitutionality of Section 2-1003(a) of the Code of Civil Procedure as amended by Public Act 89-7; 2-1003(a).[30] This statute provided that any party who

alleged a claim for bodily injury or disease was deemed to have waived any privilege of confidentiality with healthcare providers. The *Kunkel* Court recognized that Section 2-1003(a) permitted overbroad medical disclosure that circumvented the relevance requirement set forth in Rule 201(b)(1) by discouraging tort victims from pursuing valid claims because of the threat of harassment and embarrassment through unreasonable and oppressive disclosure requirements.".[31] In *Kunkel*, the Court also recognized that 2-1003(a) violated the right to privacy. The Court noted, *inter alia*, "disclosure of highly personal medical information having no bearing on the issues in the lawsuit is a substantial and unjustified invasion of privacy."[32] G.O 18-1 ignores the law as stated in *Kunkel*, which expressly forbade blanket waivers of privacy rights as to medical records in litigation.[33]

In a contemporaneous decision, *Best v. Taylor Machine Works*,[34] that Court discussed again the requirement that discovery requests be relevant to the subject matter of the litigation, and the judicial function in regulating discovery pursuant to the Supreme Court Rules.[35] The *Best* Court also reaffirmed the public policy purposes of *Petrillo v. Syntex Laboratories*,[36] recognizing that the Illinois Constitution's privacy provisions must be considered.[37] After a discussion of the purposes and policies embodied in *Petrillo*, the *Best* Court held that patients in Illinois have a privacy interest in confidential medical information, and that the *Petrillo* Court properly recognized a strong public policy in preserving patients' fiduciary and confidential relationship with his or her physicians.[38]

Personal health information is constitutionally protected. [39] Yet the G.O. 18-1 HIPAA Order is an example of an order that allows defendants and their insurance companies to gather PHI wholesale, nearly without restriction or limitation, without consideration of whether the PHI has any relevancy to the case at hand. G.O. 18-1 pits the plaintiff's right to privacy guaranteed in the Illinois Constitution[40] against the plaintiff's right to remedy and justice also guaranteed in the Illinois Constitution.[41] The legal fix to this grievous wrong is simple; the insertion of language tailored to permit dissemination only of relevant PHI.

A HIPAA order must guarantee the HIPAA privacy rules that are a floor of national protections for the minimum level of privacy for health information. The HIPAA privacy rules expressly preempt state law that permits broader access or disclosures.

Congress passed HIPAA to limit the sharing of health information and to give consumers rights to control use and disclosure of their health information at the point of disclosure. It set standards with respect to the rights of individuals who are "the subjects of this information, procedures for the exercise of those rights, and the authorized and required uses and disclosures of this information." [42] According to the Act, HIPAA preempts state law, both substantively and procedurally.[43] The statute states that any privacy "standard or implementation specification adopted or established under sections 1320d-1 through 1320d-3 of this title, shall supersede any contrary provision of State law, including a provision of State law that requires medical or health plan records (including billing information) to be maintained or transmitted in written rather than electronic form. "[44] *Id.*

The purpose of these protections was to address growing public concerns that in the age of electronic technology a substantial erosion of the privacy was likely as to PHI maintained within the health care industry.[45]

The HIPAA regulations state that "[a] standard, requirement, or implementation specification adopted under this subchapter that is contrary to a provision of State law preempts the provision of State law".[46] The HIPAA Privacy rule sets a "floor" on privacy protections but allows states to set more stringent requirements standards.[47] Far exceeding the national HIPAA floor, G.O. 18-1 HIPAA Order mandates release of nearly all of a plaintiff's PHI, regardless of relevancy; waives the plaintiff's constitutional and HIPAA rights to privacy; removes the plaintiff's right to control access to medical records; and permits auto and casualty insurance companies to use, retain, and redisclose private medical information for purposes other than litigation.

HIPAA Privacy Rules' effect on state law is contained in the statute[48] and the regulations.[49] The intent of HIPAA is "to ensure the integrity and confidentiality of patients' information and to protect against unauthorized uses or disclosures of the information." [50] Since HIPAA regulations enumerate what uses or disclosures are authorized, a court cannot add to this list to skirt HIPAA's express preemption of any provision of state law contrary to its provisions.[51]

A state law is "more stringent" than HIPAA where a "standard, requirement, or implementation…. prohibits or restricts a use or disclosure in circumstances under which such use or disclosure otherwise would be permitted under this subchapter, except if the disclosure is

made to the individual who is subject to the PHI."[52] A state law would also be "more stringent" if, "with respect to the form, substance, or the need for express legal permission from an individual who is the subject of the individually identifiable health information, or for use or disclosure of individually identifiable health information, it provides requirements that narrow the scope or duration, increase the privacy protections afforded (such as by expanding the criteria for), or reduce the coercive effect of the circumstances surrounding the express legal permission, as applicable."[53] The law would also be more stringent if it requires a longer retention and reporting of more detailed accounting of disclosures made,[54] and with respect to any matter "provides greater privacy protection for the individual who is the subject of the individually identifiable health information." [55]

As part of the American Recovery and Reinvestment Act of 2009, Congress enacted the Health Information Technology for Economic and Clinical Health Act (''the HITECH Act''). One of its main purposes was to strengthen the privacy and security protection for individuals' health information. In 2013, the Department of Health and Human Services amended its regulations implementing the HITECH Act.[56] These amendments enhanced the tools to control disclosure, use, retention, and redisclosure of health information at the point of disclosure. Under the HIPAA Privacy rules, as amended by the HITECH Act and its implementing regulations, any disclosure must comply with HIPAA either through a HIPAA-compliant court order, or a HIPAA-compliant authorization, unless the subject of health information agrees to waive protection.

Any disclosure is subject to HIPAA-conditions; the recipient of such disclosed health information is bound by the limited permissions and conditions imposed under HIPAA. The Illinois Supreme Court has not addressed HIPAA preemption with regard to medical authorization and discovery. However, the First District has recognized that HIPAA preempts state law unless the state law is more stringent.[57]

Cases from other jurisdictions have also recognized that HIPAA preempts state law. The Supreme Court of Missouri, sitting *en banc*, found that a court order which permitted communication with the plaintiff's treaters violated HIPAA. In issuing a writ of probation, the Supreme Court of Missouri observed that the "plaintiff did not issue an authorization under 45 C.F.R. § 164.508(a)(1)" but instead the trial court "issued a purported order" that the trial court believed complied with HIPAA.[58]

The Georgia Supreme Court also found that HIPAA preempts less stringent state law in the context of litigation as Georgia law was not designed to protect a patient's private health information in the course of oral communications between the patient's physicians and defense counsel."[59]

The Court of Appeals of Georgia found that HIPAA preempted a state statute that required a medical malpractice plaintiff to execute a broad medical authorization.[60] The Court noted: "Clearly, HIPAA contemplates a process in which disclosures are limited to relevant information, and a patient may object to particular disclosures that exceed the scope of the relevant inquiry. Because Georgia's statute does not limit in any way the protected health information which may be disclosed, and offers no mechanism by which a plaintiff might object to the disclosure of even completely irrelevant information, this statute does not constitute "lawful process" within the context of HIPAA." [61]

A HIPAA order that does not meet the HIPAA definition of a HIPAA court order is therefore preempted.

G.O. 18-1 uses HIPAA terminology, but itself does not meet the HIPAA criteria. HIPAA allows a medical provider or a hospital to disclose patient medical records subject to a court order.[62] HIPAA defines a HIPAA court order, limiting it in several respects.

First, the order must authorize a covered entity to disclose "only the protected information expressly authorized by such order." [63]

Second, the order must "prohibit the parties from using or disclosing the protected health information for any purpose other than the litigation or proceeding for which such information was requested;" and must require "the return to the covered entity or destruction of the protected health information (including all copies made) at the end of the litigation or proceeding."[64]

G.O. 18-1 does not satisfy the requirement in HIPAA that any PHI disclosures be "expressly authorized". Although there are no published opinions on the issue of what constitutes "expressly authorized" PHI in 45 C.F.R. § 164.512(e)(1), several federal trial courts have considered the issue and agree that the term PHI "expressly authorized" means only material relevant to the case at issue can be so authorized by a court order, and that irrelevant medical information must remain confidential. [65] It must limit the disclosure to a specific medical condition or injured body part at issue, as discussed above as a required under Illinois law.[66] Recently, the Illinois Supreme Court, in the context of whether a personal injury

defendant can assert physician-patient privilege, recognized that unless the condition is placed at issue, the records are not subject to disclosure. *Palm v. Holocker*, 2018 IL 123152, ¶ 34, reh'g denied (Jan. 10, 2019). A personal injury plaintiff's "condition at issue" would rarely be his or her entire body.

G.O. 18-1 authorizes disclosure, without express delineation, of a *"party's PHI."* To understand the extraordinary scope of such language, it is worth reviewing some of the HIPAA definitions.

"Protected health information" means "*individually identifiable information*" that is electronically transmitted or maintained electronically or in other media.[67]

"*Individually identifiable information"* is "information that is a subset of *health information*, including demographic information collected from an individual" and is "created or received by a health care provider, health plan, employer, or health care clearinghouse", and that "[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual;" and that "identifies the individual" or where "there is a reasonable basis to believe the information can be used to identify the individual."[68]

"*Health information* " means "any information" that is created by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse" and relates to "the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual."[69]

To illustrate the broad reach of an order that does not expressly delineate the PHI to be disclosed, in a hypothetical personal injury case filed by a 60-year old female plaintiff with a broken arm resulting from a rear-end collision, a defendant, defense attorneys and the defendant's insurance company can access the plaintiff's birth records, gynecological records, fertility records, breast cancer treatment records, primary care records, dental records, ophthalmology records, menstrual history records, sexual history records, breast implant records, and even records if the plaintiff had an abortion in the distant past, to name only a few of the possible medical conditions the plaintiff may have encountered during the sixty years of her life. Without limiting the PHI to a relevant condition, such an order is unconstitutionally overbroad, falls below the floor mandated by HIPAA, and is preempted by HIPAA. It forces

plaintiffs, as a condition of litigating, to waive any objection to insurance companies receiving, keeping, and using all PHI, regardless of the form of treatment, for whatever uses their business needs dictate. This too is a HIPAA violation.

To comply with HIPAA, an order must prohibit the parties from using or disclosing the PHI "for any purpose other than the litigation or proceeding for which such information was requested" and must require "the return to the covered entity or destruction of the protected health information (including all copies made) at the end of the litigation or proceeding." [70] HIPAA preempts actions by a court to expressly permit insurance companies to use a personal injury victim's PHI for their business purposes, and to retain and use the PHI beyond the conclusion of litigation.

A requirement that the personal injury victim sign a HIPAA order converts the order into an Authorization, which itself violates HIPAA and is preempted by HIPAA.

The 2018 Cook County G.O. 18-1 Order requires the plaintiff to sign the Order or face case sanctions, including dismissal, for failure to do so.[71] This coerced waiver effectively transforms the order into an authorization, a document that HIPAA regulations preempt unless it meets certain requirements, which the 2018 Order/Authorization, even signed, does not.

A valid HIPAA authorization must include core privacy elements.[72] The mandatory elements are: (i) a description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion; (ii) the name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure; (iii) the name or other specific identification of the person(s), or class of persons, to whom the covered entity may make the requested use or disclosure; (iv) a description of each purpose of the requested use or disclosure. The statement "at the request of the individual" is a sufficient description of the purpose when an individual initiates the authorization and does not, or elects not to, provide a statement of the purpose; (v) an expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure....; (vi) signature of the individual and date. If the authorization is signed by a personal representative of the individual, a description of such representative's authority to act for the individual must also be provided. The authorization also must give notice to the patient of the right to revoke the authorization.[73] In

addition to the above core elements, the Privacy Rule requires that the authorization give notice of the right to revoke the authorization in writing. [74]

A court order which forces the plaintiff to sign it as a condition of exercising her or his constitutional right to a remedy at law is both unconstitutional, and preempted by HIPAA.

HIPAA and its enacting regulations preempt any *process* to circumvent HIPAA at the state level.

To receive a HIPAA exemption when obtaining PHI in litigation, the insurance industry cannot go to a state court, but must follow federal procedure outlined in the Code of Federal Regulations.[75] The automobile, casualty, and workers' compensation insurers cannot use a court order to get an exception based on any claimed state regulatory or statutory requirements that exceed the HIPAA privacy floor. Without federally granted exceptions, any HIPAA expansion is preempted, including the G.O. 18-1 HIPAA Order.

The regulations, 45 C.F.R. § 160.204, describe the process for a State to seek a HIPAA exemption. The State's chief elected official, or his or her designee, must submit a request in writing to the Secretary.[76] The request must include: (1) the State law for which the exception is requested; (2) the particular standard, requirement, or implementation specification for which the exception is requested; (3) the part of the standard or other provision that will not be implemented based on the exception or the additional data to be collected based on the exception, as appropriate; (4) how health care providers, health plans, and other entities would be affected by the exception; (5) the reasons why the State law should not be preempted by the federal standard, requirement, or implementation specification, including how the State law meets one or more of the criteria at § 160.203(a), and (6) any other information the Secretary may request in order to make the determination.[77]

If the Secretary grants the exception based on all information provided, the exception remains in effect until there is a material change such that the grounds for the exception no longer exist, or the secretary revokes the exception based on a determination that the ground for the exception no longer exist.[78] Pursuant to responses from the Department of Health and Human Services to Freedom of Information Act requests on this issue, no applications for exemptions to permit retention and use of litigation party's protected health information have been made, let alone granted.[79]

A HIPAA Order should protect the fundamental right of privacy.

When the U.S. Department of Health and Human Services enacted the HIPAA privacy rules in 2000, it recognized that a breach of health privacy harms more than just the ability to seek medical care. The Comments to the regulations in Standards for Privacy of Individually Identifiable Health Information[80] acknowledge that a "breach of a person's health privacy can have significant implications well beyond the physical health of that person, including the loss of a job, alienation of family and friends, the loss of health insurance, and public humiliation. "[81] The comments provide several real-life examples, and others now exist with the advent of technology and digitalization.[82]

- A banker who also sat on a county health board gained access to patients' records, identified several people with cancer, and called in their mortgages.[83]
- After a physician was diagnosed with AIDS at the hospital in which he practiced, his surgical privileges were suspended.[84]
- A candidate for Congress nearly saw her campaign derailed when newspapers published the fact that she had sought psychiatric treatment after a suicide attempt. [85]
- A 30-year FBI veteran was put on administrative leave when, without his permission, his pharmacy released information about his treatment for depression.[86]

Consumer Reports found that 40 percent of insurers disclose personal health information to lenders, employers, or marketers without customer permission. [87]

To summarize the requirements by HIPAA, a HIPAA-compliant Protective Order must: (i) limit any disclosure to the health condition the plaintiff has placed at issue; (ii) forbid any subpoenas sent for "any and all" records, but instead limit the period of time for five years before the accident until the present; (iii) limit the use of the plaintiff's PHI to the litigation only, and (iv) require the return or destruction of the PHI information upon conclusion of litigation, including all appellate parties' rights.

Conclusion

Cook County General Order 18-1 was adopted because insurance companies objected to the 2012 protective order then in use by the Law Division. The trial court, in *Shull v Ellis*, properly evaluated many of the issues HIPAA orders need to address. However, the resulting order is an example of a HIPAA Order premised on critical flaws: that insurance companies are entitled to protected health information and that if they are, the belief that the Illinois Insurance

Code requires property and casualty companies to keep and maintain PHI for a period of time. According to the State of Illinois, this belief is unfounded.[88] No such rule or statute requires an insurance company to maintain PHI beyond the termination of litigation. Further, even if such a rule or statute did exist, it would still be preempted by HIPAA for expressly failing to limit the use of the PHI, and for failing to require its destruction or return upon termination of litigation. Moreover, even if such a rule or statute existed, and even if it was not preempted, there is no valid justification for allowing an insurance company to use the PHI for any purpose beyond the instant litigation at the expense of forcibly robbing a plaintiff of her constitutional and statutory rights to privacy.

The right to privacy is fundamental and is enshrined in the Illinois Constitution. Illinois courts should make every effort to protect that fundamental right. A HIPAA order cannot place the private business interests above the constitutionally guaranteed right to privacy or violate HIPAA's preemption requirements in doing so.

Cook County should reassess General Order 18-1 and draft a protective order that ensures the protections afforded by the Illinois Constitution, complies with state and federal law, including HIPAA, while allowing defendants to obtain and utilize protected health information in the defense of the case filed by the plaintiff—without permitting insurance companies to utilize that protected health information for any purpose other than for use in the instant litigation. A revised General Order could limit the time and scope of protected health information to that information relevant to any given case. Further, why should an insurance company be able to use protected health information for business uses, such as "rate setting and regulation" or "drafting policy language"? If insurance companies are to be provided protected health information there is no justifiable reason to allow them to use that protected health information for any reason beyond the instant litigation.

Another look at General Order 18-1 is in the best interests of the court and the parties that litigate there.

---

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) became effective from May 25, 2018. Available aat https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679 (Last accessed Jan. 13, 2019).

[2] *Health Insurers Are Vacuuming Up Details About You - And It Could Raise Your Rates*, https://www.propublica.org/article/health-insurers-are-vacuuming-up-details-about-you-and-it-could, ProPublica, (Last Accessed Jan. 14, 2019)
[3] O'Neil, Cathy. Weapons of math destruction: How big data increases inequality and threatens democracy. Broadway Books, 2017.
[4] *Id.*
[5] *Id.*
[6] https://scholar.google.com/scholar?hl=en&as_sdt=0%2C14&q=weapons+of+math+destruction&btnG= (last accessed Jan 13, 2019)
[7] General Administrative Order 18-1, Standard HIPAA Qualified Protective Order, entered Oct. 29, 2018, by Presiding Judge, Law Division, Judge James P. Flannery, Jr., posted at http://www.cookcountycourt.org/Portals/0/Law%20Divison/General%20Administrative%20Orders/HIPAA18-1-10292018114411%20v2.pdf
[8] *Id*.
[9] General Administrative Order 12-1, Standard HIPAA Qualified protective Order entered Sept. 19, 2012 by Presiding Judge, Law Division, William D. Maddux. Posted at http://www.cookcountycourt.org/Portals/0/Law%20Divison/General%20Administrative%20Orders/12-1%20Standard%20HIPAA%20Qualified%20Protective%20Order%20and%20Sample.PDF
[10] Mem. Op. and Order, entered Jul. 25, 2017 by Judge John H. Ehrlich, in the matter of *Shull v. Ellis* (Cook County case 15 L 975), posted at http://www.cookcountycourt.org/Portals/0/Law%20Divison/MemOpOrder/ShullMemoOpOrder25Jul17.pdf
[11] *Id*.
[12] G.O. 18-1.
[13] *Id*. These uses are: l. reporting, investigating, evaluating, adjusting, negotiating, arbitrating, litigating or settling claims; 2.compliance reporting or filing; 3. reporting criminal or lawful conduct; 4. required inspections and audits; 5. legally required reporting to private, federal or state governmental health or medical insurance organizations, including, but not limited to, the Centers for Medicare and Medicaid Services (CMS); 6. rate setting and regulation; 7. reserve and actuarial determination; 8. calculating loss; underwriting; 9. workers' compensation, and 11. determining the need for and procuring excess or umbrella coverage or reinsurance.
[14] General Administrative Order 17-4, entered December 15, 2017 by Presiding Judge, Law Division, James P. Flannery, posted at http://www.cookcountycourt.org/Portals/0/HIPAA1217-12152017092138.pdf
[15] *Id*. at 1.
[16]*Id*. at 2. These uses are: l. reporting, investigating, evaluating, adjusting, negotiating, arbitrating, litigating or settling claims; 2.compliance reporting or filing; 3.identifying and reporting criminal or lawful conduct; 4. required inspections and audits; 5. legally required reporting to private, federal or state governmental health or medical insurance organizations, including, but not limited to, the Centers for Medicare and Medicaid Services (CMS); 6. rate setting and regulation; 7. Statistical information gathering; 8. Underwriting, reserve, loss, and actuarial calculation; 9. Drafting policy language; 10. Workers' compensation, and 11. determining the need for and procuring excess or umbrella coverage or reinsurance.
[17]General Administrative Order 18-1, HIPAA Protective Order, entered Oct. 29, 2018, by Judge James P. Flannery, Presiding Judge, Law Division, Circuit Court of Cook County, Illinois, at 1. The statutes are:

> Mental Health and Developmental Disabilities Confidentiality Act, 740 ILCS 110/1- 17;
> AIDS Confidentiality Act, 410 ILCS 305/1 - 16;
> Alcoholism and Other Drug Abuse and Dependency Act, 20 ILCS 301/30-5 - 10;
> Any federal statute or regulation protecting certain drug and alcohol records, see, e.g., 42 U.S.C. §§ 290dd-3, 290ee-3; 42 C.F.R. Part 2;
> Genetic Information Privacy Act, 410 ILCS 513/15 - 50; and
> Any and all other applicable state and federal laws regulating or governing the disclosure, maintenance, use, and disposal of PHI.

[18]*Id*.at 2.
[19] *Id*. at 2 These uses are: l. reporting, investigating, evaluating, adjusting, negotiating, arbitrating, litigating or settling claims; 2.compliance reporting or filing; 3. reporting criminal or lawful conduct; 4. required inspections and audits; 5. legally required reporting to private, federal or state governmental health or medical insurance organizations, including, but not limited to, the Centers for Medicare and Medicaid Services (CMS); 6. rate setting

and regulation; 7. reserve and actuarial determination; 8. calculating loss; underwriting; 9. workers' compensation, and 11. determining the need for and procuring excess or umbrella coverage or reinsurance.
[20] Ill. Const. art. I, § 12. Constitution, Right to Remedy and Justice.
[21] Ill. Const. art. I, § 6. Constitution, Searches, Seizures, Privacy and Interceptions.
[22] U.S. Const., art. IV.
[23] 45 C.F.R. § 164.512(e)(1).
[24] *Id.*
[25] 45 C.F.R. § 164.512(e)(1)(v).
[26] 18-1 HIPAA Protective Order at 2, entered October 29, 2018, by Judge James P. Flannery, Presiding Judge, Law Division, Circuit Court of Cook County, Illinois,
[27] 18-1 HIPAA Protective Order at 5, entered October 29, 2018, by Judge James P. Flannery, Presiding Judge, Law Division, Circuit Court of Cook County, Illinois,
[28] *Firebaugh v. Traff*, 353 Ill. 82, 85 (1933).
[29] *Kunkel v. Walton*, 179 Ill.2d 519, 538 (1998).
[30] 735 ILCS 5-2/1003(a) (West 998).
[31] See *Kunkel*
[32] *Id.* at 539.
[33] *Id.*at 519.
[34] *Best v. Taylor Machine Works*, 179 Ill.2d 367 (1997).
[35] *Id.* at 446, 448.
[36] *Petrillo v. Syntex Laboratories*,[36] 148 Ill.App.3d 581(4th Dist., 1986.)
[37] *Id.* at 455.
[38] *Id.* at 458-59.
[39] *Whalen v. Roe*, 429 U.S. 589 (1977).
[40] Ill. Const. art. I, ¶ 6.
[41] Ill. Const., art. I, ¶ 12.
[42] 65 F.R. 82461, 82462 (Dec. 28, 2000).
[43] 42 U.S.C.A. § 1320d-7 (West 2018).
[44] *Id.*
[45] 65 F.R. 82461, 82462 (Dec. 28, 2000).
[46] 45 C.F.R. § 160.201.
[47] 45 C.F.R. § 160.202 (2013); see also "*Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules*", 78 FR 5566, 5690, (technical amendment showing that HIPAA Privacy Rule applies to business associates and covered entities; this rule did not alter the definition of "more stringent").
[48] 42 U.S.C.A. § 1320d-7.
[49] 45 C.F.R. § 160.201-160.205.
[50] *In re Vioxx Products Liab. Litig.*230 F.R.D. 473, 477 (E.D. La. 2005) (citing 42 U.S.C.A. § 1320d-2 (d)(2)(A), (B)(ii)).
[51] 42 U.S.C.A. § 1320d-7 (a)(1); 45 C.F.R. § 160.203.
[52] 45 C.F.R. § 160.202(a)(1).
[53] 45 C.F.R. § 160.202(a)(4).
[54] 45 C.F.R. § 160.202(a)(4).
[55] 45 C.F.R. § 160.202(a)(4).
[56] 87 F.R. 5566 (Jan 25, 2013).
[57] *Giangiulio v. Ingalls Mem'l Hosp.*, 365 Ill. App. 3d 823, 840 (1st Dist. 2006) ("HIPAA contains a preemption provision that generally supersedes contrary state law provisions. 42 U.S.C.A. § 1320d-7(a)(1) (West) (2000).")
[58] *State ex rel. Proctor v. Messina*, 320 S.W.3d 145, 154 (Mo. 2010).
[59] *Moreland v. Austin*, 284 Ga. 730, 733 (2008).
[60] In *Northlake Med. Ctr., LLC v. Queen*, 280 Ga. App. 510 (2006).
[61] *Id.* at 515.
[62] 45 C.F.R. § 164.512(e)(1)(i).
[63] 45 C.F.R. § 164.512(e)(1)(i).
[64]45 C.F.R. § 164.512(e).

[65] See, e.g., *Strayhorne v. Caruso*, CIV. 11-15216, U.S. Dist. LEXIS 30246, 2014 WL 916814, at *4, (E.D. Mich. Mar. 10, 2014) (limiting the scope of disclosure of PHI to which defense is entitled under state statue because Congress, in enacting HIPAA, recognized a societal interest in maximizing the protections in the confidential physician-patient relationship, even when a patient's medical history is at issue); *Piehl v. Saheta*, CIV. CCB-13-254, U.S. Dist. LEXIS 79401, 2013 WL 2470128, at *2 (D. Md. June 5, 2013) (interpreting the "expressly authorized" language in HPAA to permit disclosure only of material relevant to the instant case, as to do otherwise could not tailor an order to permit dissemination only of relevant facts). Illinois courts have long held that the material relevance standard is the proper one for determining relevancy of evidence in a personal injury claim. *Voykin v. Estate of DeBoer*, 192 Ill. 2d 49, 57 (2000) (requiring a causal relationship between prior and present injury for a prior injury to be admissible as relevant evidence).
[66] *Voykin*, 192 Ill. 2d at 57–58 (discussing relevancy of same body part rule); *Kunkel*, 179 Ill. 2d at 538 (discussing unreasonable invasion of privacy because of broad records disclosure requirement)
[67] 45 C.F.R. § 160.103 (Definitions).
[68] 45 C.F.R. § 160.103 (Definitions)
[69] 45 C.F.R. § 160.103 (Definitions).
[70] 45 C.F.R. § 164.512(e).
[71] G.O. 18-1 at 2
[72] 45 C.F.R. § 164.508(c)(1).
[73] 45 C.F.R. § 164.508(c)(1).
[74] 45 C.F.R. § 164.508(c)(2).
[75] 45 C.F.R. § 160.204
[76] 45 C.F.R. § 160.204(a).
[77] 45 C.F.R. § 160.204
[78] 45 C.F.R. § 160.205.
[79] Department of Health & Human Services, FOIA Case No. 2018-00901-FOIA-OS; Illinois Department of Insurance FOIA request 18-FO-0329; Illinois Department of Insurance FOIA request 18-FO-0395; Illinois Department of Public Health FOIA request 1800914885; and State of Illinois, Office of the Governor, FOIA request 2018-144.
[80] 65 FR 82462-01.
[81] *Id*.
[82] *Standards for Privacy of Individually Identifiable Health Information*, 65 FR 82462-01.
[83] See National Law Journal, May 30, 1994.
[84] See Estate of Behringer v. Med. Ctr. at Princeton, 249 N.J. Super. 597 (Law. Div. 1991).
[85] See New York Times, October 10, 1992, Section 1, page 25.
[86] Los Angeles Times, September 1, 1998.
[87] "Who's reading your Medical Records," Consumer Reports, October 1994, at 628, paraphrasing Sweeny, Latanya; "Weaving Technology and Policy Together to Maintain Confidentiality," Journal Of Law Medicine and Ethics (Summer & Fall 1997) Vol. 25, Numbers 2,3; Standards for Privacy of Individually Identifiable Health Information, 65 FR 82462-01.
[88] Department of Health & Human Services, FOIA Case No. 2018-00901-FOIA-OS; Illinois Department of Insurance FOIA request 18-FO-0329; Illinois Department of Insurance FOIA request 18-FO-0395; Illinois Department of Public Health FOIA request 1800914885; and State of Illinois, Office of the Governor, FOIA request 2018-144.

THURSDAY, APRIL 18, 2019 | SERVING CHICAGO'S LEGAL COMMUNITY FOR 164 YEARS | CHICAGOLAWBULLETIN.COM

Chicago Daily Law Bulletin®

VOLUME 165, NO. 76

LAW BULLETIN MEDIA

Court's qualified protective order form ignores HIPAA

BY ROBERT D. FINK, SOFIA ZNEIMER AND CYNTHIA S. KISSER

ROBERT D. FINK *is an attorney at Collison Law Offices, a firm that represents individuals and their families in workers' compensation, personal injury, wrongful death and catastrophic injury matters. He oversees the personal injury practice group. He can be reached at rfink@collisonltd.com.* SOFIA ZNEIMER *practices in the area of litigation and immigration. She is a member of the Order of the Coif and can be reached at sofia@zneimerlaw.com.* CYNTHIA S. KISSER *is an attorney in private practice who specializes in personal-injury law. She is a contributing author to the Illinois Continuing Legal Education 2019 edition of "Liens Under Illinois Tort Acts." She can be reached at ckisser@lhyman.com.*

An individual's medical record information, a person's most intimate personal information, cannot be understated. It has value for insurance companies and data brokers far beyond its use to settle a personal-injury claim.

As Illinois courts wrestle over privacy concerns regarding collection and use of personal data in personal-injury claims, a review is underway by the Illinois Supreme Court Rules Committee on the scope of personal health-care information courts can require plaintiffs to disclose as a condition of litigating and how these disclosures affect constitutional and federal rights to privacy.

Privacy issues surrounding the use of personal health-care information are addressed in litigation by entry of a qualified protective order. In 1996, the Health Insurance Portability and Accountability Act, or HIPAA, became federal law (42 U.S.C. Section 300gg, 29 U.S.C Section 1181, et seq., and 42 U.S.C. Section 1320d, et seq.), creating confusion in the courts as to what a qualified protective order can permit regarding disclosure of personal health-care information.

This confusion is particularly evident in the Cook County Circuit Court Law Division, where General Administrative Order 18- 1, effective Oct. 29, 2018, requires a form qualified protective order, two elements both of which directly affect the plaintiff's constitutional and federal rights to privacy.

First, the order created by General Order 18-1 requires both a plaintiff and their counsel sign the qualified protective order for the litigation to go forward. Further, it waives the plaintiff's right to privacy as to all personal health-care information, even if not related to the injury at issue.

Second, among 11 permitted uses of the disclosed personal health-care information, some not litigation-related, are the right of insurance companies to retain and use personal health-care information after the litigation has ended, even though not authorized by HIPAA to do so.

The order requires a written acknowledgment by the plaintiff that by refusing to consent to the contents of the order, the court may impose sanctions up to and including dismissal of the complaint.

This broad language violates federal, state and constitutional rights of the plaintiffs. For example, Article I, Section 12 of the Illinois Constitution guarantees all its citizens a right to access its courts to seek justice, while Section 6 guarantees them a right to privacy. Article IV of the U.S. Constitution likewise protects a citizen's right to privacy.

Yet, General Order 18-1 violates a plaintiff's privacy rights by requiring this waiver of rights to privacy to all personal health-care information as a condition of accessing the courts.

It also exceeds the authority allowed a court pursuant to Section 164.512(e) (1) of HIPAA, to disclose personal health-care information in judicial and administrative proceedings. The disclosure must be limited to specifically delineated personal health-care information expressly authorized by the order, to be used for no other purpose than the litigation, then returned or destroyed at the termination of the litigation.

The Illinois Supreme Court long ago held constitutional protections allow a court to compel the production of records only upon a proper showing that they tend to prove the issues, not for general inspection, fishing expeditions or other purposes. *Firebaugh v. Traff*, 353 Ill. 82, 85 (1933). This principle applies to the privacy interest in medical information. Kunkel v. Walton, 179 Ill.2d 519, 538 (1998). In the context of physician-patient privilege, unless a condition is placed at issue, records are not subject to disclosure. *Palm v. Holocker*, 2018 IL 123152, ¶34, reh'g denied (Jan. 10, 2019).

A personal-injury plaintiff's condition at issue cannot, therefore, generally be one's entire body of medical records. HIPAA preempts the right of a court to permit insurance companies to use personal health-care information obtained in litigation for business purposes and to retain it beyond the conclusion of litigation.

General Order 18-1 also transformed the qualified protective order into an authorization for release of personal health-care information, one that HIPAA regulations pre-empt because it does not meet certain requirements, even signed. A valid HIPAA authorization, pursuant to Section 164.508(c) (1), cannot be a blanket waiver of all personal health-care information.

It must include core privacy elements: (1) a description of the information to be used or disclosed, identified in a specific and meaningful fashion; (2) identification of the person(s) … authorized to make the requested use or disclosure; (3) identification of the person(s) … to whom the covered entity may make the requested use or disclosure; (4) a description of each purpose of the requested use or disclosure; (5) an expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure…; (6) signature of the individual and date.

General Order 18-1 is premised on a mistaken belief, articulated in the body of the form qualified protective order, that insurance companies are entitled to all of a plaintiff's personal health-care information and that the Illinois Insurance Code requires property and casualty companies to keep and maintain this personal health-care information for a period of time.

The Illinois Department of Insurance has confirmed in writing in response to a FOIA request from one of the authors that no rule or statute exists requiring an insurance company

to maintain personal health-care information beyond the termination of litigation.

Even if such a rule or statute did exist, it would still be pre-empted by HIPAA for expressly failing to limit use of the personal health-care information and require its destruction or return upon termination of litigation.

Moreover, even if such a rule or statute existed, and even if not pre-empted, there is no valid justification for allowing an insurance company to use the personal health-care information for any purpose beyond the instant litigation at the expense of forcibly robbing a plaintiff of her constitutional and statutory rights to privacy.

A HIPAA-compliant protective order must (1) limit any disclosure to the health condition the plaintiff has placed at issue; (2) forbid subpoenas for all records, and instead limit the period of time for five years before the accident until the present; (3) limit the use of the plaintiff's personal health-care information to the litigation only, and (4) require the return or destruction of the personal health-care information upon conclusion of litigation.

There must be a uniform, constitutionally sound HIPAA protective order for use in Illinois courts that protects the fundamental right to privacy of the plaintiff over private business interests which violate HIPAA's pre-emption requirements.

A qualified protective order should not pit the plaintiff's right to privacy against that plaintiff's right to remedy and justice. The legal fix to this grievous wrong is simple; the use of a qualified protective order which includes language tailored to permit dissemination only of relevant personal health-care information, and only for use in the particular litigation only.