No. 129081
IN THE ILLINOIS SUPREME COURT

LUCILLE MOSBY, Individually, and on Behalf of All Others Similarly Situated, Plaintiff-Appellee, v. THE INGALLS MEMORIAL HOSPITAL, UCM COMMUNITY HEALTH & HOSPITAL DIVISION, INC., and BECTON, DICKINSON AND COMPANY, Defendants-Appellants.	On Appeal from the Illinois Appellate Court, First District, No. 1-20-0822, No. 1-21-0895 (consol.) There on Appeal from the Circuit Court of Cook County, Illinois, County Department, Chancery Division Case No. 2018-CH-05031 The Honorable Judge Pamela McLean Meyerson Judge Presiding
YANA MAZYA, Individually, and on Behalf of All Others Similarly Situated, Plaintiff-Appellee, v. NORTHWESTERN LAKE FOREST HOSPITAL and NORTHWESTERN MEMORIAL HEALTHCARE Defendants-Appellants.	On Appeal from the Illinois Appellate Court, First District, No. 1-20-0822, No. 1-21-0895 (consol.) There on Appeal from the Circuit Court of Cook County, Illinois, County Department, Chancery Division Case No. 2018-CH-07161 The Honorable Judge Alison C. Conlon, Judge Presiding

BRIEF OF *AMICUS CURIAE* ILLINOIS HEALTH AND HOSPITAL ASSOCIATION IN SUPPORT OF DEFENDANTS-APPELLANTS

E-FILED
5/8/2023 2:20 PM
CYNTHIA A. GRANT
SUPREME COURT CLERK

Michael A. Scodro
David S. Levine
MAYER BROWN LLP
71 S. Wacker Dr.
Chicago, Illinois 60606
(312) 782-0600
mscodro@mayerbrown.com
dlevine@mayerbrown.com

Counsel for Amicus Curiae

TABLE OF CONTENTS AND POINTS AND AUTHORITIES

INTEREST OF THE *AMICUS CURIAE*

The Illinois Health and Hospital Association ("IHA") represents over 200 hospitals and 40 health systems throughout the State of Illinois. Member hospitals include community hospitals, urban hospitals, safety net hospitals, specialty hospitals, rural and critical access hospitals, as well as teaching and academic medical centers. For over 80 years, IHA has served as an advocate for these members, addressing the social, economic, political, and legal issues affecting the delivery of high-quality health care in Illinois. IHA's purpose is, among other things, to support each person's quest for optimum health and to ensure that all individuals and communities have access to high-quality health care at the right time and in the right setting. In pursuing this purpose, IHA routinely advocates for rules that strengthen hospitals and improve the quality of care provided to their patients.

This appeal will significantly impact IHA's members. As described below, this appeal concerns whether an exclusion under the Illinois Biometric Information Privacy Act ("BIPA" or the "Act") applies to biometric information of health care workers (as opposed to patients) where that information is collected, used, or stored for health care treatment, payment, or operations under the Health Insurance Portability and Accountability Act ("HIPAA"). Given the importance of this issue to IHA's members, IHA submitted an amicus brief in this case before the Illinois Appellate Court, First District ("First District"), which the First District accepted.

This appeal will play a critical role in hospitals' decisions regarding the technologies they deploy in providing health care to Illinois residents. Relatedly, the appeal will also have an important impact on the potential liability of many Illinois health care providers—a concern only exacerbated by recent decisions expanding liability under BIPA. *See Cothron v. White Castle Sys., Inc.*, 2023 IL 128004; *Tims v. Black Horse Carriers, Inc.*, 2023 IL 127801. Indeed, as discussed further below, should the Court adopt Plaintiffs' interpretation of the Act, IHA's members would likely confront an onslaught of astronomical damages claims and often would elect not to use the important technologies at issue in this case. Given these and other implications, IHA has a significant interest in this appeal.

INTRODUCTION

BIPA provides that "[b]iometric identifiers do not include information captured from a patient in a health care setting or *information collected, used, or stored for health care treatment, payment, or operations under the federal Health Insurance Portability and Accountability Act of 1996*." 740 ILCS 14/10 (emphasis added). This case presents the important question of whether the italicized language refers exclusively to *patient* information.

IHA agrees with Defendants-Appellants that the plain text, structure, and purpose of the statute demonstrate that the exclusion is not so confined and also exempts a health care worker's "information collected, used, or stored for health care treatment, payment, or operations under the federal Health Insurance Portability and Accountability Act of 1996." 740 ILCS 14/10. As

Justice Mikva explained in dissent below, the "General Assembly *did* intend to exclude from the Act's protections the biometric information of healthcare workers—including finger-scan information collected by those workers' employers—where that information is collected, used, or stored for health care treatment, payment, or operations, as those functions are defined by HIPAA." *See Mosby v. Ingalls Mem'l Hosp.*, 2022 IL App (1st) 200822, ¶ 74 ("Opinion") (Mikva, J., Dissenting). Plaintiffs' and the majority's interpretation, Justice Mikva continued, "ignore important rules of statutory construction, while overcomplicating a more straightforward reading of this exclusion." *Id.*

IHA submits this brief to emphasize additional considerations supporting this conclusion. As described below, the Act instructs in multiple sections that it should be interpreted consistently with HIPAA. That makes good sense. From the time of the Act's passage to today, HIPAA regulations and related guidance have encouraged health care workers to use biometric authentication, and the plain language of Section 14/10 prevents BIPA from conflicting with these federal determinations. In contrast, Plaintiffs' interpretation would interfere squarely with federal health care policy and regulations. Plaintiffs' reading would lead to astronomical liability for hospitals merely following federal guidance, and it would cause many providers to discontinue the use of federally recommended technologies intended to promote patient care and public safety more broadly. That result

runs contrary to the Act's interpretive instructions and provides an additional reason for rejecting Plaintiffs' interpretation.

BACKGROUND

This consolidated appeal involves two cases brought by nurses advancing individual and putative class claims under BIPA in connection with their use of medication-dispensing systems.

These systems promote the secure administration of medications and medical supplies used to treat patients. To obtain access to the medications, medical supplies, and associated protected health information in the system's electronic interface, a health care worker first self-identifies by entering a user name, then scans their finger to authenticate that self-identification.[1] As described further in Defendants-Appellants' brief, these systems play an important role in controlling access to prescription medications, including controlled substances such as valium, morphine, and fentanyl. The systems also reduce medication errors, maintain an audit trail to detect diversion, fraud, and abuse, and allow hospitals to ensure proper billing for medication and medical supplies. Studies also suggest that these systems increase the efficiency of health care workers and improve patient care.[2]

---

[1] As the First District noted, Defendants-Appellants deny that these medication dispensing systems collect, store, or use a biometric identifier or biometric information as those terms are defined by BIPA. *See* Opinion ¶ 46 n.7. That issue is not relevant to this appeal.

[2] *See, e.g.*, Hanne Katriina Ahtiainen *et al.*, *Safety, time and cost evaluation of automated and semi- automated drug distribution systems in hospitals: a systematic review*, Eur. J. Hosp. Pharm. (Sept. 2020) (concluding

In both cases in this consolidated appeal, the defendants moved to dismiss the complaints on the basis of BIPA's exemption for "information collected, used, or stored for health care treatment, payment, or operations under the federal Health Insurance Portability and Accountability Act of 1996." *See* Opinion ¶¶ 2, 10, 22. The circuit courts denied the motions, and in the consolidated certified appeal pursuant to Rule 308, the Appellate Court, First District, concluded "that the biometric information of health care workers is not excluded under the Act." *Id.* ¶ 5. Justice Mikva dissented, and this Court granted a petition for leave to appeal. *See Mosby v. Ingalls Mem'l Hosp.*, 460 Ill.Dec. 584 (2023).

ARGUMENT

This Court should interpret the exclusion to cover the biometric information of health care workers where that information is collected, used, or stored for health care treatment, payment, or operations, as those functions are defined by HIPAA. In addition to the exclusion's plain language and other factors, that conclusion follows from a consideration of the exclusion in light of HIPAA's regulations pertaining to biometric authentication.

---

that medication dispensing systems "improved medication safety and quality of care, mainly by decreasing medication errors"); Riikka Metsämuuronen *et al.*, *Nurses' Perceptions of Automated Dispensing Cabinets – An Observational Study and an Online Survey*, 19 BMC Nursing J. 27 (Apr. 2020) ("Nearly 80% of the nurses in the ICU and 42% in the OR found that [medication-dispensing devices] make their work easier. The observational study revealed that in the OR, time spent on dispensing and preparing medications decreased on average by 32 min per 8-h shift and more time was spent on direct patient care activities.").

In particular, in the years preceding BIPA's passage, federal regulators promulgated rules and issued guidance pursuant to HIPAA encouraging the use of biometric authentication by health care workers. Against that backdrop, the General Assembly sensibly included language limiting any interference with HIPAA by requiring that BIPA be interpreted consistently with HIPAA and its associated regulations.

Plaintiffs' interpretation would upset this balance. Under Plaintiffs' construction of the Act, entities covered by HIPAA—such as the hospital defendants in this appeal and IHA's members[3]—would be forced to choose between following federal recommendations or facing astronomical liability. Undoubtedly, many entities would choose to discontinue the authentication devices despite federal regulators' judgment that these devices promote patient wellbeing and public safety. Because this result would be contrary to the text of BIPA and the purpose of the Section 14/10 exclusion, Plaintiffs' interpretation should be rejected.

Part I, below, explains why BIPA must be interpreted consistently with HIPAA. Part II details HIPAA rules and recommendations related to biometric authentication. And Part III describes why Plaintiffs' interpretation would cause health care providers, now facing astronomical liability, to break from

[3] *See*, *e.g.*, *Pesoli v. Dep't of Employment Sec.*, 2012 IL App (1st) 111835, ¶ 31 (noting that health care providers like hospitals are covered entities under HIPAA).

these federal recommendations and would thus run afoul of the principles discussed in Part I.

I. The Act Should Be Interpreted Consistently With HIPAA.

In passing BIPA, the General Assembly made clear that the statute should be interpreted consistently with HIPAA. This requirement is reflected in two provisions of the Act and also accords with the Act's purposes.

The first provision appears in the section of BIPA detailing how the statute should be interpreted. *See* 740 ILCS 14/25 ("Construction"). This section contains broad exemptions for certain financial institutions, state agencies, and other entities, and the section then states: "Nothing in this Act shall be construed to conflict with . . . [HIPAA] and the rules promulgated under [HIPAA]." *Id.* 14/25(b).

The rules promulgated under HIPAA are then the focus of the second provision, the one at issue in this appeal. That exclusion provides that "[b]iometric identifiers do not include . . . information collected, used, or stored for health care treatment, payment, or operations under the federal Health Insurance Portability and Accountability Act of 1996." 740 ILCS 14/10. As Justice Mikva explained, health care "treatment, payment and operations" are "terms of art that are carefully and explicitly defined in HIPAA's implementing regulations." Opinion ¶ 78 (Mikva, J. Dissenting).[4] Not only do HIPAA

[4] HIPAA defines "health care" broadly to include "care, services, or supplies related to the health of an individual," including the "[s]ale or dispensing of a drug, device, equipment, or other item in accordance with a prescription." 45 C.F.R. § 160.103. "Treatment" is defined to include any

regulations expressly define those terms, moreover, but the "triumvirate of healthcare treatment, payment, and operations is repeatedly used" throughout HIPAA regulations "to define the activities of covered entities that are the subject of those regulations." Opinion ¶ 80 (Mikva, J. Dissenting).[5]

The General Assembly's instruction to interpret the Act consistently with HIPAA, and even more pointedly to use terms defined by HIPAA in an exclusion, makes good sense. In passing the Act, the General Assembly recognized that biometric technology has tremendous potential for good. *See, e.g.*, 740 ILS 14/5(a) (describing benefits of "streamlined financial transactions and security screenings" from biometric authentication); *see also Vance v. Amazon.com Inc.*, 534 F. Supp. 3d 1314, 1322 (W.D. Wash. 2021) (noting that Illinois "legislature recognized the benefits of using biometrics" in passing

---

activity that involves "the provision, coordination, or management of health care and related services by one or more health care providers." 45 C.F.R. § 164.501. "Payment" includes "activities undertaken by . . . [a] health care provider or health plan to obtain or provide reimbursement for the provision of health care." *Id.* And "[h]ealth care operations" includes, among other things, "patient safety activities," "general administrative activities of the entity," and conducting or arranging for "auditing functions, including fraud and abuse detection and compliance programs." *Id.*

[5] *See id.* ("45 C.F.R. § 164.506 (titled 'Uses and disclosures to carry out treatment, payment, or health care operations' and employing the phrase 'treatment, payment, or health care operations' an additional seven times); *id.* § 164.502 (using the phrase twice); *id.* § 164.504 (using the phrase three times); *id.* § 164.508 (using the phrase once); *id.* § 164.514 (using the phrase once); *id.* § 164.520 (using the phrase twice); *id.* § 164.522 (using the phrase twice); *id.* § 164.528 (using the phrase once); *id.* § 170.210 (using the phrase twice); and *id.* § 170.315 (using the phrase once)").

BIPA). And these potential benefits include the use of biometric authentication for "health care treatment, payment, or operations." 740 ILCS 14/10.

As further described below, these health care applications were already the subject of federal regulation under HIPAA at the time of BIPA's passage. *See infra* Part II. Thus, rather than interfere with this federal regulation, the General Assembly instructed that BIPA be interpreted consistently with HIPAA and therefore, as one legislator noted, provided "exemptions as necessary for hospitals." *See* H.R. 95-276, Gen. Assemb., at 249 (Ill daily ed. May 30, 2008) (statement of Rep. Ryg); *see also People v. Lowe*, 153 Ill.2d 195, 203 (1992) (analyzing "[s]tatements of representatives considering" proposed statute "in order to establish legislative intent"); *Bogseth v. Dr. B. Emanuel*, 261 Ill.App.3d 685, 690 (1st Dist. 1994) ("An effective means of ascertaining the intent underlying specific legislation is to analyze the legislative history, including debates of legislators conducted on the floor of the General Assembly.").

II. HIPAA Encourages The Use Of Biometric Authentication By Health Care Workers.

HIPAA regulations and related guidance encourage the use of biometric authentication by health care workers. HIPAA's stated purpose is to, among other things, "combat waste, fraud, and abuse in . . . health care delivery." Pub. L. No. 104–191, 110 Stat. 1936 (1996). The Department of Health and Human Services (the "Department") implements HIPAA and has promulgated

regulations to effectuate this purpose. *See Giangiulio v. Ingalls Mem'l Hosp*., 365 Ill. App. 3d 823, 839 (1st Dist. 2006).

Since before BIPA was passed, the Department has recommended that health care entities covered by HIPAA use fingerprints or other biometrics for authorization and authentication purposes. In 2003, for example, the Department issued the "Security Rule," providing that covered entities must, among other things, implement policies and procedures to limit "access to its electronic information systems." *Health Insurance Reform: Security Standards*, 68 FR 8334-01 (Feb. 20, 2003). Specifically, the Security Rule provides that covered entities should implement procedures to "control . . . access to software programs" and to safeguard "equipment" at the hospital from "unauthorized physical access, tampering, and theft." *Id.* at 8378. Even more pointedly, the regulation requires covered entities to "[i]mplement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed." *Id*. at 8379.[6]

[6] These provisions remain in effect today. *See, e.g.*, 45 C.F.R. § 164.310(a)(1) (providing that covered entities must implement policies and procedures to limit "access to its electronic information systems"); *id.* § 164.310(a)(2)(ii) (providing that a covered entity should implement "policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft"); *id*. § 164.310(a)(2)(iii) (providing that a covered entity should implement procedures "to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision"); *id*. § 164.312(d) (requiring that covered entities "[i]mplement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed").

In the years that followed, and shortly before BIPA's passage, the Department issued guidance elaborating on these requirements and expressly recommended the use of biometric authentication by health care workers and other hospital staff. In 2006, for example, the Department "strongly urged" covered entities to implement authorization and authentication procedures, including "the use of biometrics, such as fingerprint readers, on portable devices."[7] In additional guidance the following year, the Department again recommended that to "authenticate" a particular employee or staff member, covered entities under HIPAA "require something unique to the individual such as a biometric. Examples of biometrics include fingerprints, voice patterns, facial patterns or iris patterns."[8] And in 2008—the year of BIPA's passage—the National Institute of Standards and Technology issued its own guidelines in connection with the Security Rule and recommended that covered entities use "some type of biometric identification . . . such as a fingerprint" for authentication purposes.[9] As noted, these recommendations relate to

---

[7] *HIPAA Security Guidance* at 5, Dep't of Health and Human Servs. (Dec. 28, 2006).

[8] *HIPAA Security Series* at 10, Dep't of Health and Human Servs. (Mar. 2007).

[9] *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule* at 46, Dep't of Commerce, Nat'l Inst. of Standards and Tech. (Oct. 2008). NIST "is responsible for developing standards and guidelines, including minimum requirements, used by federal agencies in providing adequate information security for the protection of agency operations and assets." *Id.* at 1. Its "publications serve as a valuable resource for federal agencies, as well as

authentication *of health care workers* and other hospital staff—not patients—and indicate that the use of biometric authentication in the health care setting is not just permitted, but favored, as a means of implementing HIPAA's goals.

Thus, at the time of BIPA's passage, federal regulation already existed with respect to the use of biometric authentication by health care workers. Against that backdrop, the General Assembly included an express exemption for "information collected, used, or stored for health care treatment, payment, or operations" under HIPAA and made clear that "[n]othing in this Act shall be construed to conflict" with HIPAA or "the rules promulgated" under HIPAA. 740 ILCS 14/10, 14/25. But as described in the next part, Plaintiffs' interpretation of the exclusion would do just that.

III. Plaintiffs' Interpretation Would Result In Providers Discontinuing These Recommended Technologies And Thus Put BIPA In Conflict With HIPAA Regulations.

Plaintiffs' construction of the Act would result in astronomical liability for providers following the guidance provided by federal HIPAA regulations. Confronted with this potential liability, many providers would simply discontinue use of these technologies that studies suggest improve patient care and that federal regulators expressly recommend. Because this result would create conflict between the two statutes and thus violate BIPA's interpretive instructions, Plaintiffs' construction of the Act should be rejected.

---

public, nonfederal agencies and private organizations, seeking to address existing and new federal information security requirements." *Id*.

Consider the choice faced by a health care provider under Plaintiffs' construction of BIPA. Although federal regulations plainly favor the use of biometric authentication, following this federal guidance—designed by health care regulators to protect patients and the public—could subject providers to overwhelming liability under BIPA. Given the many patients that they treat every shift, health care professionals often must provide authentication multiple times per day, if not per hour. Covered entities also typically have multiple dispensing systems on site, and each system might be used hundreds or even thousands of times per week. And of course these providers operate every hour of every day, 365 days per year.

The need for such constant, immediate access to medications could easily lead to astronomical BIPA liability capable of bankrupting many hospitals. Consider a putative class of, say, 150 nurses who on average provide their authentication five times per day and work 200 days per year. Assume also that the nurses claim—as Plaintiff Mazya does here, Opinion ¶ 19—that each authentication results in at least two alleged violations of the statute. These assumptions are extremely conservative given, among other things, the number of staff and patients at Illinois hospitals and the ordinary use of these medication dispensing systems.[10] Yet even with these modest assumptions, the

[10] For example, a supplier of a single brand of medication dispensing systems—Omnicell—recently reached a class action settlement under BIPA that involves a class of nearly 60,000 users. *See Heard v. Omnicell, Inc.*, Case No. 2019 CH 6817, at 6 (Cir. Ct. Cook County, Mar. 23, 2023) (Plaintiff's Unopposed Motion for Final Approval of Class Action Settlement). This large

hospital would face $1.5 billion in BIPA exposure.[11] An award of this magnitude would at a minimum cause hospitals to divert significant resources away from patient care and could even lead some into bankruptcy.

It is no response to say that these health care providers need only comply with the statute to avoid this exposure. Much of the statute remains subject to judicial interpretation. What qualifies as a "fingerprint" (740 ILCS 14/10), what it means to "otherwise profit from" biometric data (740 ILCS 14/15(c)), and the precise contours of "informed written consent" (740 ILCS 14/10) are just a few of the many questions that have not been conclusively answered.

From a compliance perspective, moreover, health care providers face unique challenges. For one, many users of the authentication devices—such as emergency medical services (EMS) personnel and individuals from staffing agencies—are *non*-employees of the providers. As a result, health care providers cannot simply rely on employee onboarding processes to ensure

---

class size is unsurprising both given the ubiquity of these devices and given that, according to one recent report, approximately 1 in 10 Illinois jobs are in health care. *See* Illinois Health and Hospital Association, *Illinois Hospitals and Health Systems: Crucial for Community Health and Economic Stability* (2022). Indeed, as of 2021, Northwestern Memorial Health Care alone employed 29,800 physicians, nurses, allied health professionals, clinical support staff and administrative employees. *See* Opinion ¶ 64 n.13 (quoting amicus brief). In fiscal year 2020, moreover, the Northwestern health system had more than 104,000 inpatient admissions and more than 2.2 million outpatient encounters. *See id.*

[11] This example conservatively assumes $1,000 per violation, with 150 nurses alleging 10 violations per day, 200 days per year, for the five-year limitations period. That is, 1000*150*10*200*5.

compliance—instead, enrolling non-employees such as EMS and temporary staff on these devices is a separate process, often completed right as they are deployed. What's more, these individuals are regularly using the devices under trying and time-sensitive circumstances where seconds can mean the difference between a patient living or dying. Under these conditions, health care providers cannot delay the treatment process to confirm that a particular user has indeed executed a written consent.[12]

Even a fully compliant hospital, moreover, would face significant challenges in litigating a putative class action under BIPA. That is because these high-exposure claims, even if meritless, are very difficult to defeat without expensive discovery. Even if the plaintiff concedes that she signed a BIPA-compliant consent, for example, fact questions may remain regarding the circumstances of the consent (e.g., whether it preceded the scan) and the treatment of the collected data (e.g., whether and how it was shared with a third party). As new technologies emerge, the problems with applying BIPA's requirements will only become more acute. For instance, a particular technology may only appear to capture biometric information—but expensive

[12] Not only do *patient* emergencies result in the urgent use of these medication-dispensing devices, but *staffing* emergencies can as well. Staffing shortages in the health care industry are well known and a "top patient safety concern." *See, e.g.*, Steven Ross Johnson, *Staff Shortages Choking U.S. Health Care System*, U.S. News & World Report (July 28, 2022). As a result of these shortages, nurses and other personnel are often sent to hospitals by outside agencies on extremely short notice and with little or no time for onboarding given urgent patient needs.

discovery would still likely be needed to establish that the technology does not in fact do so. *See, e.g.*, *In re Facebook Biometric Info. Priv. Litig.*, 2018 WL 2197546, at *2 (N.D. Cal. May 14, 2018) ("While the parties have no serious disagreement about the literal text of Facebook's source code, they offer strongly conflicting interpretations of how the software processes human faces.").

Plaintiffs' interpretation of Section 14/10 thus would result in tremendous potential for *in terrorem* settlements by defendants acting pursuant to federal guidance but facing immense exposure under BIPA. These *in terrorem* settlements are a serious problem recognized by the judicial system. As the U.S. Supreme Court has observed, faced "with even a small chance of a devastating loss, defendants will be pressured into settling questionable claims." *AT&T Mobility LLC v. Concepcion*, 563 U.S. 333, 350 (2011); *see also Shady Grove Orthopedic Assocs., P.A. v. Allstate Ins. Co.*, 559 U.S. 393, 445 n.3 (2010) (Ginsburg, J., dissenting) ("When representative plaintiffs seek statutory damages, [the] pressure to settle may be heightened because a class action poses the risk of massive liability unmoored to actual injury."); *In re Rhone–Poulenc Rorer Inc.*, 51 F.3d 1293, 1297-98 (7th Cir. 1995) ("Judge Friendly, who was not given to hyperbole, called settlements induced by a small probability of an immense judgment in a class action 'blackmail settlements.' Judicial concern about them is legitimate . . . ." (citation omitted)).

For many health care providers, this confluence of factors—astronomical exposure, unique compliance challenges, and the prospect of *in terrorem* settlements—would cause the providers to discontinue the use of these recommended technologies under HIPAA. Because this result would run afoul of BIPA's interpretive instructions discussed above—depriving patients and the public of the recognized benefits of these technologies in the provision of health care, *see, e.g.*, *supra* p. 4 n.2—Plaintiffs' construction of the Act should be rejected.

CONCLUSION

For the reasons set forth above and in the brief of Defendants-Appellants, the Court should hold that BIPA excludes from the definition of "biometric identifiers" a health care worker's information collected, used, or stored for health care treatment, payment, or operations under HIPAA.

Dated: April 26, 2023

Respectfully submitted,

/s/ Michael A. Scodro

Michael A. Scodro
David S. Levine
MAYER BROWN LLP
71 S. Wacker Dr.
Chicago, Illinois 60606
(312) 782-0600
mscodro@mayerbrown.com
dlevine@mayerbrown.com

Counsel for Amicus Curiae

Supreme Court Rule 341(c) Certificate of Compliance

I certify that this brief conforms to the requirements of Rule 341(a) and (b). The length of this brief, excluding the pages or words contained in the Rule 341(d) cover, the Rule 341(h)(1) table of contents and statement of points and authorities, the Rule 341(c) certificate of compliance, the certificate of service, and those matters appended to the brief under Rule 342(a) is 17 pages.

/s/Michael A. Scodro
Michael A. Scodro
Mayer Brown LLP