Douglas S. Swetnam (IN State Bar #15860-49)
Section Chief – Data Privacy & ID Theft Unit
Office of Attorney General Curtis Hill Jr.
302 W. Washington St., 5th Floor
Indianapolis, IN 46204
Email: douglas.swetnam@atg.in.gov
Telephone: (317) 232-6294

Michael A. Eades (IN State Bar #31015-49)
Deputy Attorney General
Office of Attorney General Curtis Hill, Jr.
302 W. Washington St., 5th Floor
Indianapolis, IN 46204
Email: Michael.Eades@atg.in.gov
Telephone: (317) 234-6681

Taylor C. Byrley (IN State Bar #35177-49)
Deputy Attorney General
Office of Attorney General Curtis Hill Jr.
302 W. Washington St., 5th Floor
Indianapolis, IN 46204
Email: Taylor.Byrley@atg.in.gov
Telephone: (317) 234-2235
Attorneys for Plaintiff State of Indiana

John C. Gray (Pro Hac Vice)
Assistant Attorney General
Office of Attorney General Mark Brnovich
2005 N. Central Ave.
Phoenix, AZ 85004
Email: John.Gray@azag.gov
Telephone: (602) 542-7753
Attorney for Plaintiff State of Arizona

Peggy Johnson (Pro Hac Vice)
Assistant Attorney General
Office of Attorney General Leslie Rutledge
323 Center St., Suite 200
Little Rock, AR 72201
Email: peggy.johnson@arkansasag.gov
Telephone: (501) 682-8062
Attorney for Plaintiff State of Arkansas

Diane Oates (Pro Hac Vice)
Assistant Attorney General
Office of Attorney General Pam Bondi
110 Southeast 6th Street
Fort Lauderdale, FL 33301
Email: Diane.Oates@myfloridalegal.com
Telephone: (954) 712-4603
Attorney for Plaintiff State of Florida

William Pearson (Pro Hac Vice)
Assistant Attorney General
Office of Attorney General Tom Miller
1305 E. Walnut, 2nd Floor
Des Moines, IA 50319
Email: William.Pearson@ag.iowa.gov
Telephone: (515) 281-3731
Attorney for Plaintiff State of Iowa

Sarah Dietz (Pro Hac Vice)
Assistant Attorney General
Office of Attorney General Derek Schmidt
120 S.W. 10th Ave., 2nd Floor
Topeka, KS 66612
Email: sarah.dietz@ag.ks.gov
Telephone: (785) 368-6204
Attorney for Plaintiff State of Kansas

Kevin R. Winstead (Pro Hac Vice)
Assistant Attorney General
Office of Attorney General Andy Beshear
1024 Capital Center Drive
Frankfort, KY 40601
Email: Kevin.Winstead@ky.gov
Telephone: (502) 696-5389
Attorney for Plaintiff Commonwealth of Kentucky

Alberto A. De Puy (Pro Hac Vice)
Assistant Attorney General
Office of Attorney General Jeff Landry
1885 N. Third St.
Baton Rouge, LA 70802
Email: DePuyA@ag.louisiana.gov
Telephone: (225) 326-6471

L. Christopher Styron (Pro Hac Vice)
Assistant Attorney General
Office of Attorney General Jeff Landry
1885 N. Third St.
Baton Rouge, LA 70802
Email: styronl@ag.louisiana.gov
Telephone: (225) 326-6400
Attorneys for Plaintiff State of Louisiana

Jason T. Pleggenkuhle (Pro Hac Vice)
Assistant Attorney General
Office of Attorney General Lori Swanson
Bremer Tower, Suite 1200
445 Minnesota St.
St. Paul, MN 55101-2130
Email: jason.pleggenkuhle@ag.state.mn.us
Telephone: (651) 757-1147
Attorney for Plaintiff State of Minnesota

Daniel J. Birdsall (Pro Hac Vice)
Assistant Attorneys General
Office of Attorney General Doug Peterson
2115 State Capitol
PO Box 98920
Lincoln, NE 68509
Email: dan.birdsall@nebraska.gov
Telephone: (402) 471-1279
Attorney for Plaintiff State of Nebraska

Kimberley A. D'Arruda (Pro Hac Vice)
Special Deputy Attorney General
North Carolina Department of Justice
Office of Attorney General Joshua H. Stein
P.O. Box 629
Raleigh, NC 27602-0629
Email: kdarruda@ncdoj.gov
Telephone: (919) 716-6013
Attorney for Plaintiff State of North Carolina

Lara Sutherlin (Pro Hac Vice)
Wisconsin Department of Justice
Office of Attorney General Brad Schimel
17 W. Main St., P.O. Box 7857
Madison, WI 53707-7857
Email: sutherlinla@doj.state.wi.us
Telephone: (608) 267-7163
Attorney for Plaintiff State of Wisconsin

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF INDIANA

The States of Arizona; Arkansas; Florida; Indiana; Iowa; Kansas; Kentucky; Louisiana; Minnesota; Nebraska; North Carolina; and Wisconsin, Plaintiffs; vs. Medical Informatics Engineering, Inc. d/b/a Enterprise Health, LLC and K&L Holdings, and NoMoreClipboard, LLC, Defendants.	Case No.: **COMPLAINT**

COMPLAINT

Plaintiffs, the states of Arizona, Arkansas, Florida, Indiana, Iowa, Kansas, Kentucky, Louisiana, Minnesota, Nebraska, North Carolina, and Wisconsin (collectively "Plaintiff States"), for their complaint against Defendants Medical Informatics Engineering, Inc., ("MIE") operating as Enterprise Health, LLC and K&L Holdings, and NoMoreClipboard, LLC, ("NMC" together with MIE "Defendants"), allege:

SUMMARY OF THE CASE

1. Intermittently between May 7, 2015 and May 26, 2015, unauthorized persons ("hackers") infiltrated and accessed the inadequately protected computer systems of Defendants. During this time, the hackers were able to access and exfiltrate the electronic Protected Health Information ("ePHI"), as defined by 45 C.F.R. § 160.103, of 3.9 million individuals, whose PHI was contained in an electronic medical record stored in Defendants' computer systems. Such personal information obtained by the hackers included names, telephone numbers, mailing

addresses, usernames, hashed passwords, security questions and answers, spousal information (names and potentially dates of birth), email addresses, dates of birth, and Social Security Numbers. The health information obtained by the hackers included lab results, health insurance policy information, diagnosis, disability codes, doctors' names, medical conditions, and children's name and birth statistics.

2. In fostering a security framework that allowed such an incident to occur, Defendants failed to take adequate and reasonable measures to ensure their computer systems were protected, failed to take reasonably available steps to prevent the breaches, failed to disclose material facts regarding the inadequacy of their computer systems and security procedures to properly safeguard patients' personal health information, failed to honor their promises and representations that patients' personal health information would be protected, and failed to provide timely and adequate notice of the incident, which caused significant harm to consumers across the United States.

3. Defendants' actions resulted in the violation of the state consumer protection, data breach, personal information protection laws and federal HIPAA statutes, as more fully outlined below. Plaintiffs seek to enforce said laws by bringing this action.

4. This action is brought, in their representative and individual capacities as provided by state and federal law, by the attorneys general of Arizona, Arkansas, Florida, Indiana, Iowa, Kansas, Kentucky, Louisiana, Minnesota, Nebraska, North Carolina, and Wisconsin (collectively the "Attorneys General"). The plaintiffs identified in the paragraph are also referred to collectively as the "Plaintiff States."

5. The Plaintiff States bring this action pursuant to consumer protection, business regulation, and/or data security oversight authority conferred on their attorneys general,

secretaries of state, and/or state agencies by state law, federal law, and/or pursuant to *parens patriae* and/or common law authority. These state laws authorize the Plaintiff States to seek temporary, preliminary, and permanent injunctive relief, civil penalties, attorneys' fees, expenses, costs, and such other relief to which the Plaintiff States may be entitled.

6. This action is also brought by the Attorneys General of the Plaintiff States pursuant to the Health Insurance Portability and Accountability Act of 1996, as amended by the Health Information Technology for Economic and Clinical Health ("HITECH") Act, 42 U.S.C. § 1302(a), and the Department of Health and Human Services Regulations, 45 C.F.R. § 160 *et seq.*(collectively, "HIPAA"), which authorize attorneys general to initiate federal district court proceedings and seek to enjoin violations of, and enforce compliance with HIPAA, to obtain damages, restitution, and other compensation, and to obtain such further and other relief as the court may deem appropriate.

JURISDICTION AND VENUE

7. This Court has jurisdiction over the federal law claims pursuant to 42 U.S.C. § 1320d-5(d), and 28 U.S.C. §§ 1331 and 1337(a). This Court has supplemental jurisdiction over the subject matter of the state law claims pursuant to 28 U.S.C. § 1367.

8. Venue in this District is proper pursuant to 28 U.S.C. §§ 1391(b) and (c).

9. The Attorneys General provided prior written notice of this action to the Secretary of HHS, as required by 42 U.S.C. § 1320d-5(d)(4). The Attorneys General have also provided a copy of this complaint to the Secretary of HHS. *Id.*

10. At all times relevant to this matter, Defendants were engaged in trade and commerce affecting consumers in the States insofar as Defendants provided electronic health

records services to health care providers in the States. Defendants also maintained a website for patients and client health care providers in the States.

PLAINTIFFS

11. The Attorneys General are charged with, among other things, enforcement of the Deceptive Trade Practices Acts, the Personal Information Protection Acts, and the Breach Notification Acts. The Attorneys General, pursuant to 42 U.S.C. § 1320d-5(d), may also enforce HIPAA.

12. The Attorneys General are the chief legal officers for their respective states and commonwealths. The Plaintiff States bring this action pursuant to consumer protection, business regulation, and/or data security oversight authority conferred on their attorneys general, secretaries of state, and/or state agencies by state law, federal law, and/or pursuant to *parens patriae* and/or common law authority.

13. Plaintiff Attorneys General institute this action for injunctive relief, statutory damages, attorney fees, and the costs of this action against Defendants for violations of the Health Insurance Portability and Accountability Act of 1996, as amended by the Health Information Technology for Economic and Clinical Health ("HITECH") Act, 42 U.S.C. § 1302(a), and the Department of Health and Human Services Regulations, 45 C.F.R. § 160 *et seq.*(collectively, "HIPAA"), and supplemental state law claims under Plaintiffs' respective Unfair, Deceptive, or Abusive Acts or Practices ("UDAP") statutes, Disclosure of Data Breach Statutes (also referred to as "Breach Notification Acts"), and Personal Information Protection Statutes (also referred to as "PIPA"), specifically:

State	Deceptive Acts	Data Breach	PIPA
Arizona:	Ariz. Rev. Stat. § 44-1521 et seq.		
Arkansas:	Ark. Code § 4-88-101 *et seq.*	Ark. Code § 4-110-105	Ark. Code § 4-110-101 *et seq.*
Florida:	Chapter 501, Part II, Florida Statutes	Section 501.171, Florida Statutes	Section 501.171(9), Florida Statutes
Indiana:	Ind. Code §§ 24-5-0.5-4(C), and 24-5-0.5-4(G)		Ind. Code § 24-4.9-3-3.5(f)
Iowa:	Iowa Code § 714.16	Iowa Code § 715c.2	
Kansas:	Kan. Stat. §§ 50-632, and 50-636	Kan. Stat. § 50-7a02	Kan. Stat. § 50-6139b
Kentucky:	Ky. Rev. Stat. §§ 367.110-.300, and 367.990		
Louisiana:	La. Rev. Stat. § 51:1401 et seq.	La. Rev. Stat. 51:3071 et seq.	
Minnesota:	Minn. Stat. §§ 325D.43 *et seq.*; Minn. Stat. §§ 325F.68 *et seq.*	Minn. Stat. § 325E.61	
Nebraska:	Neb. Rev. Stat. §§ 59-1602; 59-1608, 59-1614, and 87-301	Neb. Rev. Stat. § 87-806	
North Carolina	N.C. Gen. Stat. § 75-1.1, *et seq*.	N.C. Gen. Stat. § 75-65	N.C. Gen. Stat. § 75-60, *et seq*.
Wisconsin:	Wis. Stat. §§ 93.20, 100.18, and 100.26	Wis. Stat. § 134.98	Wis. Stat. §§ 146.82 and 146.84(2)(b)

DEFENDANTS

14. Defendant MIE is a citizen of the State of Indiana. MIE is a corporation that is incorporated in Indiana and has its principal place of business in Indiana at 6302 Constitution Drive, Fort Wayne, IN 46804.

15. Defendant NMC is a citizen of the State of Indiana. NMC is a wholly-owned subsidiary of MIE, is organized in Indiana, and has its principal place of business in Indiana at 6312 Constitution Drive, Fort Wayne, IN 46804.

16. Prior to January 6, 2016, MIE also operated under the name of Enterprise Health. Enterprise Health was a division of MIE. On January 6, 2016, MIE formed Enterprise Health, LLC, which shares founders, officers, employees, offices, and servers with MIE and NMC.

17. K&L Holdings, LLC is affiliated with MIE and has the same founders, officers, and occupies the same offices as MIE, NMC, and Enterprise Health. K&L Holdings, LLC owns the property that serves as the headquarters for K&L Holdings, LLC, MIE, NMC, and Enterprise Health.

FACTUAL ALLEGATIONS

18. MIE is a third-party provider that licenses a web-based electronic health record application, known as WebChart, to healthcare providers. MIE, through its subsidiary NMC, also provides patient portal and personal health records services to healthcare providers that enable patients to access and manage their electronic health records. Through its WebChart application, MIE provides electronic health services to physicians and medical facilities nationwide.

19. At all relevant times, MIE's customers consisted of healthcare providers who were Covered Entities within the meaning of HIPAA. 45 C.F.R. § 160.103.

20. At all relevant times, MIE and NMC were Business Associates within the meaning of HIPAA. 45 C.F.R. § 160.103.

21. As Business Associates, Defendants are required to comply with the HIPAA federal standards that govern the security of ePHI, including Security Rules. *See* 45 C.F.R. § 164.302.

22. The Security Rule generally prohibits Covered Entities and Business Associates, such as Defendants, from unlawfully disclosing ePHI. The Security Rule requires Covered Entities and Business Associates to employ appropriate Administrative, Physical, and Technical Safeguards to maintain the security and integrity of ePHI. *See* 45 C.F.R. § 164.302.

23. At all relevant times, no written agreement existed between MIE and its subsidiary NMC to appropriately safeguard the information created, received, maintained, or transmitted by the entities.

24. Between May 7, 2015 and May 26, 2015, hackers infiltrated and accessed the computer systems of Defendants.

25. The hackers stole the ePHI of 3.9 million individuals whose health information was contained in an electronic medical records database stored on Defendants' computer systems.

26. On June 10, 2015, MIE announced a "data security compromise that has affected the security of some personal and protected health information relating to certain clients and individuals who have used a Medical Informatics Engineering electronic health record." *Medical Informatics Engineering Updates Notice to Individuals of Data Security Compromise,* MIE (July 23, 2015), http://www.mieweb.com/notice.

27. On June 20, 2015, NMC announced "a data security compromise that has affected the security of some personal and protected health information relating to individuals who have used a NoMoreClipboard personal health record or patient portal." *NoMoreClipboard Notice to Individuals of a Data Security Compromise*, NoMoreClipboard (July 23, 2015), https://www.nomoreclipboard.com/notice.

28. Defendants admitted that unauthorized access to their network began on May 7, 2015, but they did not discover the suspicious activity until May 26, 2015.

29. After discovering the intrusion, Defendants "began an investigation to identify and remediate any identified security vulnerability," hired "a team of third-party experts to investigate the attack and enhance data security and protection," and "reported this incident to law enforcement including the FBI Cyber Squad." *MIE Notice*, http://www.mieweb.com/notice; *NoMoreClipboard Notice*, https://www.nomoreclipboard.com/notice.

30. MIE admitted that the following information was accessed by the hackers: "an individual's name, telephone number, mailing address, username, hashed password, security question and answer, spousal information (name and potentially date of birth), email address, date of birth, Social Security number, lab results, health insurance policy information, diagnosis, disability code, doctor's name, medical conditions, and child's name and birth statistics." *MIE Notice*, http://www.mieweb.com/notice.

31. NMC admitted that the following information was accessed by the hackers: "an individuals' [sic] name, home address, Social Security number, username, hashed password, spousal information (name and potentially date of birth), security question and answer, email address, date of birth, health information, and health insurance policy information." *NoMoreClipboard Notice*, https://www.nomoreclipboard.com/notice.

32. Defendants began notifying affected individuals by mail on July 17, 2015. This was two months after the initial breach date of May 7, 2015, and over 50 days after the breach discovery date of May 26, 2015.

33. Defendants did not conclude mailing notification letters until December 2015, six months after the breach discovery date of May 26, 2015.

34. Defendants' security framework was deficient in several respects. Defendants failed to implement basic industry-accepted data security measures to protect individual's health information from unauthorized access. Specifically, Defendants set up a generic "tester" account which could be accessed by using a shared password called "tester" and a second account called "testing" with a shared password of "testing". In addition to being easily guessed, these generic accounts did not require a unique user identification and password in order to gain remote access. In a formal penetration test conducted by Digital Defense in January 2015, these accounts were identified as high risk, yet Defendants continued to employ the use of these accounts and, in fact, acknowledged establishing the generic accounts at the request of one of its' health care provider clients so that employees did not have to log-in with a unique user identification and password.

35. Defendants did not have appropriate security safeguards or controls in place to prevent exploitation of vulnerabilities within their system. The "tester" account did not have privileged access but did allow the attacker to submit a continuous string of queries, known as a SQL injection attack, throughout the database as an authorized user. The queries returned error messages that gave the intruder hints as to why the entry was incorrect, providing valuable insight into the database structure.

36. The vulnerability to an SQL injection attack was identified as a high risk during a penetration test performed by Digital Defense in 2014. Digital Defense recommended that Defendant "take appropriate measures to implement the use of parameterized queries, or ensure the sanitization of user input." Despite this recommendation, Defendants took no steps to remedy the vulnerability.

37. The intruder used information gained from the SQL error messages to access the "checkout" account, which had administrative privileges. The "checkout" account was used to

access and exfiltrate more than 1.1 million patient records from Defendants' databases. The SQL error exploit was also used to obtain a second privileged account called "dcarlson". The "dcarlson" account was used to access and exfiltrate more than 565,000 additional records that were stored in a database containing NMC patient records.

38. On May 25, 2015, the attacker initiated a second method of attack by inserting malware called a "c99" cell on Defendants' system. This malware caused a massive number of records to be extracted from Defendants' databases. The huge document dump slowed down network performance to such an extent that it triggered a network alarm to the system administrator. The system administrator investigated the event and terminated the malware and data exfiltration on May 26, 2015.

39. Defendant's post-breach response was inadequate and ineffective. While the c99 attack was being investigated, the attacker continued to extract patient records on May 26 and May 28, using the privileged "checkout" credentials acquired through use of the SQL queries. On those two days, a total of 326,000 patient records were accessed.

40. The breach was not successfully contained until May 29, when a security contractor hired by Defendant identified suspicious IP addresses which led the contractor to uncover the principal SQL attack method.

41. Defendants failed to implement and maintain an active security monitoring and alert system to detect and alert on anomalous conditions such as data exfiltration, abnormal administrator activities, and remote system access by unfamiliar or foreign IP addresses. The significance of the absence of these security tools cannot be overstated, as two of the IP addresses used to access Defendants' databases originated from Germany. An active security

operations system should have identified remote system access by an unfamiliar IP address and alerted a system administrator to investigate.

42. Defendants' privacy policy, in effect at the time of the breach, stated: "Medical Informatics Engineering uses encryption and authentication tools (password and user identification) to protect your personal information…[O]ur employees are aware that certain information provided by our customers is confidential and is to be protected." Yet Defendants failed to encrypt the sensitive personal information and ePHI within MIE's computer systems, a protection that, had it been employed, would have rendered the data unusable.

43. Defendants' information security policies were deficient and poorly documented. For example, the incident response plan provided by Defendants was incomplete. There are several questions posed in the document that indicate it is still in a coordination or draft stage. Indeed, there is no documented evidence or checklist to indicate that Defendants followed their own incident response plan. Finally, there is no documentation that Defendants conducted HIPAA Security and Awareness training for 2013, 2014, or 2015, prior to the breach.

44. Defendants' actions caused harm to members of the Plaintiff States. Specifically, the victims are subject to emotional distress due to their personal information and ePHI being in the hands of unknown and untrusted individuals, in addition to the increased potential for harm that could result from instances of fraud.

DEFENDANTS' LAW VIOLATIONS

Count I
Arizona: Violation of HIPAA Safeguards

45. Plaintiff, Arizona, incorporates the factual allegations in paragraphs 1 through 44 of this Complaint.

46. Defendants' conduct constitutes violations of Administrative Safeguards, Technical Safeguards, and implementation specifications as required by HIPAA. Specifically:

a. MIE failed to review and modify security measures needed to continue the provision of reasonable and appropriate protection of ePHI in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.306(e).

b. MIE failed to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI that it maintained in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(A).

c. MIE failed to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(B).

d. MIE failed to implement procedures to regularly review records of information system activity, such as audit logs, access reports, and Security Incident tracking reports in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D).

e. MIE failed to implement policies and procedures that, based upon its access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process that includes ePHI in accordance with 45 C.F.R. § 164.308(a)(4)(ii)(C).

f. MIE failed to implement policies and procedures to address Security Incidents, including suspected Security Incidents, to mitigate, to the extent practicable, harmful effects of security incidents known to MIE, or to document such Incidents and their outcomes in accordance with the implementation specifications of the Security Rule, 45 C.F.R. § 164.308(a)(6)(ii).

g. MIE failed to assign a unique name and/or number for identifying and tracking user identity in accordance with the implementation specifications of the Security Rule. 45 C.F.R. § 164.312(a)(2)(i).

h. MIE failed to implement a mechanism to encrypt and decrypt ePHI, in accordance with the implementation specifications of the Security Rule. 45 C.F.R. § 164.312(a)(2)(iv).

i. MIE failed to implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI, in violation of 45 C.F.R. § 164.312(b).

j. MIE failed to implement procedures to verify that a person or entity seeking access to ePHI is the one claimed, in violation of 45 C.F.R. § 164.312(c)(2)(d).

k. MIE failed to adhere to the Minimum Necessary Standard when using or disclosing ePHI, in violation of 45 C.F.R. § 164.502(b)(1).

47. Plaintiff, Arizona, is entitled to certain statutory damages pursuant to 42 U.S.C. 1320d-5(d)(2).

Count II
Arizona: Violation of Ariz. Rev. Stat. § 44-1522

48. Plaintiff, Arizona, incorporates the factual allegations in paragraphs 1 through 44 of this Complaint.

49. The Defendants' conduct constitutes a violation of Ariz. Rev. Stat. § 44-1522.

50. The information security failings outlined in paragraphs 30 through 40 constitute unfair or deceptive acts in violation of Ariz. Rev. Stat. § 44-1522.

51. For example, MIE committed unfair or deceptive acts or practices by representing, in connection with the advertisement and sale of its services, that it maintained appropriate Administrative and Technical Safeguards to protect patients' ePHI and other appropriate measures to protect consumers' sensitive information, when such was not the case.

52. Defendants' security failings were also likely to cause substantial injury to consumers, including identity theft, and such injury was not reasonably avoidable by the consumers themselves, particularly in light of Defendants' failure to notify consumers in the most expedient manner possible, nor would such injury be outweighed by any countervailing benefits to consumers or competition.

53. Defendants' conduct was also willful, as, among other things, they knew or should have known that their unfair or deceptive acts or practices were unlawful.

54. Plaintiff, Arizona, is entitled to injunctive relief, restitution to all affected persons, and disgorgement of Defendants' profits or revenues obtained by means of its unlawful conduct pursuant to Ariz. Rev. Stat. § 44-1528; civil penalties pursuant to Ariz. Rev. Stat. § 44-1531; and attorney fees and costs pursuant to Ariz. Rev. Stat. § 44-1534.

Count III
Arkansas: Violation of HIPAA Safeguards

55. Plaintiff, Arkansas, incorporates the factual allegations in paragraphs 1 through 44 of this Complaint.

56. Defendants' conduct constitutes violations of Administrative Safeguards, Technical Safeguards, and implementation specifications as required by HIPAA. Specifically:

a. MIE failed to review and modify security measures needed to continue the provision of reasonable and appropriate protection of ePHI in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.306(e).

b. MIE failed to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI that it maintained in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(A).

c. MIE failed to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(B).

d. MIE failed to implement procedures to regularly review records of information system activity, such as audit logs, access reports, and Security Incident tracking reports in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D).

e. MIE failed to implement policies and procedures that, based upon its access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process that includes ePHI in accordance with 45 C.F.R. § 164.308(a)(4)(ii)(C).

f. MIE failed to implement policies and procedures to address Security Incidents, including suspected Security Incidents, to mitigate, to the extent practicable, harmful effects of security incidents known to MIE, or to document such Incidents and

their outcomes in accordance with the implementation specifications of the Security Rule, 45 C.F.R. § 164.308(a)(6)(ii).

g. MIE failed to assign a unique name and/or number for identifying and tracking user identity in accordance with the implementation specifications of the Security Rule. 45 C.F.R. § 164.312(a)(2)(i).

h. MIE failed to implement a mechanism to encrypt and decrypt ePHI, in accordance with the implementation specifications of the Security Rule. 45 C.F.R. § 164.312(a)(2)(iv).

i. MIE failed to implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI, in violation of 45 C.F.R. § 164.312(b).

j. MIE failed to implement procedures to verify that a person or entity seeking access to ePHI is the one claimed, in violation of 45 C.F.R. § 164.312(c)(2)(d).

k. MIE failed to adhere to the Minimum Necessary Standard when using or disclosing ePHI, in violation of 45 C.F.R. § 164.502(b)(1).

57. Plaintiff, Arkansas, is entitled to certain statutory damages pursuant to 42 U.S.C. 1320d-5(d)(2).

Count IV
Arkansas: Deceptive Acts in Violation of Ark. § 4-88-101

58. Plaintiff, Arkansas, incorporates the factual allegations in paragraphs 1 through 44 of this Complaint.

59. The Defendants' conduct constitutes a violation of Ark. Code § 4-88-108.

60. The information security failings outlined in paragraphs 30 through 40 constitute unfair or deceptive acts in violation of Ark. Code § 4-88-108.

61. MIE committed an unfair or deceptive act by representing that it maintained appropriate Administrative and Technical Safeguards to protect patients' ePHI, and other appropriate measures to protect consumers' sensitive information, when such was not the case, in violation of Ark. Code Ann. § 4-88-107(b) and Ark. Code Ann. § 4-88-108.

62. Plaintiff, Arkansas, is entitled to civil penalties pursuant to Ark. Code § 4-88-113(a)(3), attorney's fees and costs pursuant to Ark. Code § 4-88-113(e), and injunctive relief pursuant to Ark. Code § 4-88-113(a)(1).

Count V
Arkansas: Data Breach Violation of Ark. Code § 4-110-105

63. Plaintiff, Arkansas, incorporates the factual allegations in paragraphs 1 through 44 of this Complaint.

64. MIE failed to notify affected individuals or others of the Data Breach as required by Ark. Code § 4-110-105.

65. As alleged in paragraphs 28 and 29, Defendants began notifying affected individuals on July 17, 2015 and did not conclude until December 2015. The effective notice date range after the breach was discovered was between 52 days and six months.

66. By waiting between 52 days and six months to notify affected individuals, Defendants violated Ark. Code § 4-110-105.

67. Plaintiff, Arkansas, is entitled to civil penalties pursuant to Ark. Code §§ 4-110-108, 4-88-113(a)(3), attorney fees and costs pursuant to Ark. Code §§ 4-110-108, 4-88-113(e), and injunctive relief pursuant to Ark. Code §§ 4-110-108, 4-88-113(a)(1).

Count VI
Arkansas: Failure to Implement Reasonable Procedures to Protect Personal Information in Violation of Ark. Code § 4-110-104(b)

68. Plaintiff, Arkansas, incorporates the factual allegations in paragraphs 1 through 44 of this Complaint.

69. Defendants failed to implement and maintain reasonable procedures to protect and safeguard the unlawful disclosure of personal information in violation of Ark. Code § 4-110-104(b).

70. The information security failings outlined in paragraphs 30 through 40 constitute unreasonable safeguard procedures in violation of Ark. Code § 4-110-104(b).

71. Plaintiff, Arkansas, is entitled to civil penalties pursuant to Ark. Code §§ 4-110-108, 4-88-113(a)(3), attorney fees and costs pursuant to Ark. Code §§ 4-110-108, 4-88-113(e), and injunctive relief pursuant to Ark. Code §§ 4-110-108, 4-88-113(a)(1).

Count VII
Florida: Violation of HIPAA Safeguards

72. Plaintiff, Florida, incorporates the factual allegations in paragraphs 1 through 44 of this Complaint.

73. Defendants' conduct constitutes violations of Administrative Safeguards, Technical Safeguards, and implementation specifications as required by HIPAA. Specifically:

a. MIE failed to review and modify security measures needed to continue the provision of reasonable and appropriate protection of ePHI in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.306(e).

b. MIE failed to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI

that it maintained in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(A).

c. MIE failed to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(B).

d. MIE failed to implement procedures to regularly review records of information system activity, such as audit logs, access reports, and Security Incident tracking reports in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D).

e. MIE failed to implement policies and procedures that, based upon its access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process that includes ePHI in accordance with 45 C.F.R. § 164.308(a)(4)(ii)(C).

f. MIE failed to implement policies and procedures to address Security Incidents, including suspected Security Incidents, to mitigate, to the extent practicable, harmful effects of security incidents known to MIE, or to document such Incidents and their outcomes in accordance with the implementation specifications of the Security Rule, 45 C.F.R. § 164.308(a)(6)(ii).

g. MIE failed to assign a unique name and/or number for identifying and tracking user identity in accordance with the implementation specifications of the Security Rule. 45 C.F.R. § 164.312(a)(2)(i).

h. MIE failed to implement a mechanism to encrypt and decrypt ePHI, in accordance with the implementation specifications of the Security Rule. 45 C.F.R. § 164.312(a)(2)(iv).

i. MIE failed to implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI, in violation of 45 C.F.R. § 164.312(b).

j. MIE failed to implement procedures to verify that a person or entity seeking access to ePHI is the one claimed, in violation of 45 C.F.R. § 164.312(c)(2)(d).

k. MIE failed to adhere to the Minimum Necessary Standard when using or disclosing ePHI, in violation of 45 C.F.R. § 164.502(b)(1).

74. Plaintiff, Florida, is entitled to certain statutory damages pursuant to 42 U.S.C. 1320d-5(d)(2).

Count VIII
Florida: Deceptive Acts in Violation of Section 501.204, Florida Statutes

75. Plaintiff, Florida, incorporates the factual allegations in paragraphs 1 through 44 of this Complaint.

76. The Defendants' conduct constitutes a violation of Section 501.204, Florida Statutes.

77. The information security failings outlined in paragraphs 30 through 40 constitute unfair or deceptive acts in violation of Section 501.204, Florida Statutes.

78. MIE committed an unfair or deceptive act by representing that it maintained appropriate Administrative and Technical Safeguards to protect patients' ePHI, and other appropriate measures to protect consumers' sensitive information, when such was not the case, in violation of Section 501.204, Florida Statutes.

79. Plaintiff, Florida, is entitled to civil penalties pursuant to Section 501.2075, Florida Statutes, attorney fees and costs pursuant to Section 501.2105, Florida Statutes, and injunctive relief pursuant to Section 501.207(b), Florida Statutes.

Count IX
Florida: Data Breach Violation of Section 501.171, Florida Statutes

80. Plaintiff, Florida, incorporates the factual allegations in paragraphs 1 through 44 of this Complaint.

81. MIE failed to notify affected individuals or others of the Data Breach as required by Section 501.171(4), Florida Statutes.

82. As alleged in paragraphs 28 and 29, Defendants began notifying affected individuals on July 17, 2015 and did not conclude until December 2015. The effective notice date range after the breach was discovered was between 52 days and six months.

83. By waiting between 52 days and six months to notify affected individuals, Defendants violated Section 501.171(4), Florida Statutes.

84. Plaintiff, Florida, is entitled to civil penalties pursuant to Section 501.171(9), Florida Statutes, attorney fees and costs pursuant to Section 501.171(9), Florida Statutes and injunctive relief pursuant to Section 501.171(9), Florida Statutes.

Count X
Florida: Failure to Implement Reasonable Procedures to Protect Personal Information in Violation of Section 501.171(2), Florida Statutes

85. Plaintiff, Florida, incorporates the factual allegations in paragraphs 1 through 44 of this Complaint.

86. Defendants failed to implement and maintain reasonable procedures to protect and safeguard the unlawful disclosure of personal information in violation of Section 501.171(2), Florida Statutes.

87. The information security failings outlined in paragraphs 30 through 40 constitute unreasonable safeguard procedures in violation of Section 501.171(4), Florida Statutes.

88. Plaintiff, Florida, is entitled to civil penalties pursuant to Section 501.171(9)(b), Florida Statutes, attorney fees and costs pursuant to Section 501.171(9), Florida Statutes and injunctive relief pursuant to Section 501.171(9), Florida Statutes.

Count XI
Indiana: Violation of HIPAA Safeguards

89. Plaintiff, Indiana, incorporates the factual allegations in paragraphs 1 through 44 of this Complaint.

90. Defendants' conduct constitutes violations of Administrative Safeguards, Technical Safeguards, and implementation specifications as required by HIPAA. Specifically:

a. MIE failed to review and modify security measures needed to continue the provision of reasonable and appropriate protection of ePHI in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.306(e).

b. MIE failed to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI that it maintained in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(A).

c. MIE failed to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(B).

d. MIE failed to implement procedures to regularly review records of information system activity, such as audit logs, access reports, and Security Incident tracking reports in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D).

e. MIE failed to implement policies and procedures that, based upon its access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process that includes ePHI in accordance with 45 C.F.R. § 164.308(a)(4)(ii)(C).

f. MIE failed to implement policies and procedures to address Security Incidents, including suspected Security Incidents, to mitigate, to the extent practicable, harmful effects of security incidents known to MIE, or to document such Incidents and their outcomes in accordance with the implementation specifications of the Security Rule, 45 C.F.R. § 164.308(a)(6)(ii).

g. MIE failed to assign a unique name and/or number for identifying and tracking user identity in accordance with the implementation specifications of the Security Rule. 45 C.F.R. § 164.312(a)(2)(i).

h. MIE failed to implement a mechanism to encrypt and decrypt ePHI, in accordance with the implementation specifications of the Security Rule. 45 C.F.R. § 164.312(a)(2)(iv).

i. MIE failed to implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI, in violation of 45 C.F.R. § 164.312(b).

j. MIE failed to implement procedures to verify that a person or entity seeking access to ePHI is the one claimed, in violation of 45 C.F.R. § 164.312(c)(2)(d).

k. MIE failed to adhere to the Minimum Necessary Standard when using or disclosing ePHI, in violation of 45 C.F.R. § 164.502(b)(1).

91. Plaintiff, Indiana, is entitled to certain statutory damages pursuant to 42 U.S.C. 1320d-5(d)(2).

Count XII
Indiana: Deceptive Acts in Violation of Ind. Code § 24-5-0.5-3

92. Plaintiff, Indiana, incorporates the factual allegations in paragraphs 1 through 44 of this Complaint.

93. The Defendants' conduct constitutes a violation of Ind. Code § 24-5-0.5-3.

94. The information security failings outlined in paragraphs 30 through 40 constitute unfair or deceptive acts in violation of Ind. Code § 24-5-0.5-3.

95. MIE committed an unfair or deceptive act by representing that it maintained appropriate Administrative and Technical Safeguards to protect patients' ePHI, and other appropriate measures to protect consumers' sensitive information, when such was not the case, in violation of Ind. Code § 24-5-0.5-3.

96. Plaintiff, Indiana, is entitled to civil penalties pursuant to Ind. Code § 24-5-0.5-4(g), attorney fees and costs pursuant to Ind. Code § 24-5-0.5-4(c), and injunctive relief pursuant to Ind. Code § 24-5-0.5-4(c).

Count XIII
Indiana: Failure to Implement Reasonable Procedures to Protect Personal Information in Violation of Ind. Code § 24-4.9-3-3.5

97. Plaintiff, Indiana, incorporates the factual allegations in paragraphs 1 through 44 of this Complaint.

98. Defendants failed to implement and maintain reasonable procedures to protect and safeguard the unlawful disclosure of personal information in violation of Ind. Code § 24-4.9-3-3.5(c).

99. The information security failings outlined in paragraphs 30 through 40 constitute unreasonable safeguard procedures in violation of Ind. Code § 24-5-0.5-3.5.

100. Defendants are not exempt from Ind. Code § 24-5-0.5-3.5, as the Defendants did not comply with a HIPAA compliancy plan. Ind. Code § 24-5-0.5-3.5(a)(6).

101. Plaintiff, Indiana, is entitled to civil penalties pursuant to Ind. Code § 24-4.9-3-3.5(f)(2), attorney fees and costs pursuant to Ind. Code § 24-4.9-3-3.5(f)(3), and injunctive relief pursuant to Ind. Code § 24-4.9-3-3.5(f)(1).

Count XIV
Iowa: Violation of HIPAA Safeguards

102. Plaintiff, Iowa, incorporates the factual allegations in paragraphs 1 through 44 of this Complaint.

103. Defendants' conduct constitutes violations of Administrative Safeguards, Technical Safeguards, and implementation specifications as required by HIPAA. Specifically:

a. MIE failed to review and modify security measures needed to continue the provision of reasonable and appropriate protection of ePHI in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.306(e).

b. MIE failed to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI that it maintained in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(A).

c. MIE failed to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(B).

d. MIE failed to implement procedures to regularly review records of information system activity, such as audit logs, access reports, and Security Incident tracking reports in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D).

e. MIE failed to implement policies and procedures that, based upon its access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process that includes ePHI in accordance with 45 C.F.R. § 164.308(a)(4)(ii)(C).

f. MIE failed to implement policies and procedures to address Security Incidents, including suspected Security Incidents, to mitigate, to the extent practicable, harmful effects of security incidents known to MIE, or to document such Incidents and their outcomes in accordance with the implementation specifications of the Security Rule, 45 C.F.R. § 164.308(a)(6)(ii).

g. MIE failed to assign a unique name and/or number for identifying and tracking user identity in accordance with the implementation specifications of the Security Rule. 45 C.F.R. § 164.312(a)(2)(i).

h. MIE failed to implement a mechanism to encrypt and decrypt ePHI, in accordance with the implementation specifications of the Security Rule. 45 C.F.R. § 164.312(a)(2)(iv).

i. MIE failed to implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI, in violation of 45 C.F.R. § 164.312(b).

j. MIE failed to implement procedures to verify that a person or entity seeking access to ePHI is the one claimed, in violation of 45 C.F.R. § 164.312(c)(2)(d).

k. MIE failed to adhere to the Minimum Necessary Standard when using or disclosing ePHI, in violation of 45 C.F.R. § 164.502(b)(1).

104. Plaintiff, Iowa, is entitled to certain statutory damages pursuant to 42 U.S.C. 1320d-5(d)(2).

Count XV
Iowa: Deceptive Acts in Violation of Iowa Code § 714.16

105. Plaintiff, Iowa, incorporates the factual allegations in paragraphs 1 through 44 of this Complaint.

106. The Defendants' conduct constitutes a violation of Iowa Code § 714.16.

107. The information security failings outlined in paragraphs 30 through 40 constitute unfair or deceptive acts in violation of Iowa Code § 714.16.

108. MIE committed an unfair or deceptive act by representing that it maintained appropriate Administrative and Technical Safeguards to protect patients' ePHI, and other appropriate measures to protect consumers' sensitive information, when such was not the case, in violation of Iowa Code § 714.16.

109. Plaintiff, Iowa, is entitled to civil penalties pursuant to Iowa Code § 714.16(8), attorney fees and costs pursuant to Iowa Code § 714.16(11), and injunctive relief pursuant to Iowa Code § 714.16(7).

Count XVI
Iowa: Data Breach Violation of Iowa Code § 715C.2

110. Plaintiff, Iowa, incorporates the factual allegations in paragraphs 1 through 44 of this Complaint.

111. MIE failed to notify affected individuals or others of the Data Breach as required by Iowa Code § 715C.2.

112. As alleged in paragraphs 28 and 29, Defendants began notifying affected individuals on July 17, 2015 and did not conclude until December 2015. The effective notice date range after the breach was discovered was between 52 days and six months.

113. By waiting between 52 days and six months to notify affected individuals, Defendants violated Iowa Code § 715C.2.

114. Plaintiff, Iowa, is entitled to civil penalties pursuant to Iowa Code §§ 715C.2(9), 714.16(7), attorney fees and costs pursuant to Iowa Code §§ 715C.2(9), 714.16(7), and injunctive relief pursuant to Iowa Code §§ 715C.2(9), 714.16(7).

Count XVII
Kansas: Violation of HIPAA Safeguards

115. Plaintiff, Kansas, incorporates the factual allegations in paragraphs 1 through 44 of this Complaint.

116. Defendants' conduct constitutes violations of Administrative Safeguards, Technical Safeguards, and implementation specifications as required by HIPAA. Specifically:

a. MIE failed to review and modify security measures needed to continue the provision of reasonable and appropriate protection of ePHI in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.306(e).

b. MIE failed to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI that it maintained in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(A).

c. MIE failed to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(B).

d. MIE failed to implement procedures to regularly review records of information system activity, such as audit logs, access reports, and Security Incident tracking reports in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D).

e. MIE failed to implement policies and procedures that, based upon its access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process that includes ePHI in accordance with 45 C.F.R. § 164.308(a)(4)(ii)(C).

f. MIE failed to implement policies and procedures to address Security Incidents, including suspected Security Incidents, to mitigate, to the extent practicable, harmful effects of security incidents known to MIE, or to document such Incidents and their outcomes in accordance with the implementation specifications of the Security Rule, 45 C.F.R. § 164.308(a)(6)(ii).

g. MIE failed to assign a unique name and/or number for identifying and tracking user identity in accordance with the implementation specifications of the Security Rule. 45 C.F.R. § 164.312(a)(2)(i).

h. MIE failed to implement a mechanism to encrypt and decrypt ePHI, in accordance with the implementation specifications of the Security Rule. 45 C.F.R. § 164.312(a)(2)(iv).

i. MIE failed to implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI, in violation of 45 C.F.R. § 164.312(b).

j. MIE failed to implement procedures to verify that a person or entity seeking access to ePHI is the one claimed, in violation of 45 C.F.R. § 164.312(c)(2)(d).

k. MIE failed to adhere to the Minimum Necessary Standard when using or disclosing ePHI, in violation of 45 C.F.R. § 164.502(b)(1).

117. Plaintiff, Kansas, is entitled to certain statutory damages pursuant to 42 U.S.C. 1320d-5(d)(2).

Count XVIII
Kansas: Deceptive Acts in Violation of Kan. Stat. § 50-626

118. Plaintiff, Kansas, incorporates the factual allegations in paragraphs 1 through 44 of this Complaint.

119. The Defendants' conduct constitutes a violation of Kan. Stat. § 50-626**.**

120. The information security failings outlined in paragraphs 30 through 40 constitute unfair or deceptive acts in violation of Kan. Stat. § 50-626.

121. MIE committed an unfair or deceptive act by representing that it maintained appropriate Administrative and Technical Safeguards to protect patients' ePHI, and other

appropriate measures to protect consumers' sensitive information, when such was not the case, in violation of Kan. Stat. § 50-626.

122. Plaintiff, Kansas, is entitled to civil penalties pursuant to Kan. Stat. § 50-636, attorney fees and costs pursuant to Kan. Stat. § 50-632(a)(4), and injunctive relief pursuant to Kan. Stat. § 50-632(a)(2).

Count XIX
Kansas: Data Breach Violation of Kan. Stat. § 50-7a02

123. Plaintiff, Kansas, incorporates the factual allegations in paragraphs 1 through 44 of this Complaint.

124. MIE failed to notify affected individuals or others of the Data Breach as required by Kan. Stat. § 50-7a02.

125. As alleged in paragraphs 28 and 29, Defendants began notifying affected individuals on July 17, 2015 and did not conclude until December 2015. The effective notice date range after the breach was discovered was between 52 days and six months.

126. By waiting between 52 days and six months to notify affected individuals, Defendants violated Kan. Stat. § 50-7a02.

127. Plaintiff, Kansas, is entitled to appropriate relief pursuant Kan. Stat. § 50-7a02(g).

Count XX
Kansas: Failure to Implement Reasonable Procedures to Protect Personal Information in Violation of Kan. Stat. § 50-6139b(b)(1)

128. Plaintiff, Kansas, incorporates the factual allegations in paragraphs 1 through 44 of this Complaint.

129. Defendants failed to implement and maintain reasonable procedures to protect and safeguard the unlawful disclosure of personal information in violation of Kan. Stat. § 50-6139b(b)(1).

130. The information security failings outlined in paragraphs 30 through 40 constitute unreasonable safeguard procedures in violation of Kan. Stat. § 50-6139b(b)(1).

131. Plaintiff, Kansas, is entitled to civil penalties pursuant to Kan. Stat. §§ 50-6139b(d, e), 50-636, attorney fees and costs pursuant to Kan. Stat. §§ 50-6139b(d, e), 50-636(c), and injunctive relief pursuant to Kan. Stat. §§ 50-6139b(d, e), 50-632(a)(2).

Count XXI
Kentucky: Violation of HIPAA Safeguards

132. Plaintiff, Kentucky, incorporates the factual allegations in paragraphs 1 through 44 of this Complaint.

133. Defendants' conduct constitutes violations of Administrative Safeguards, Technical Safeguards, and implementation specifications as required by HIPAA. Specifically:

a. MIE failed to review and modify security measures needed to continue the provision of reasonable and appropriate protection of ePHI in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.306(e).

b. MIE failed to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI that it maintained in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(A).

c. MIE failed to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(B).

d. MIE failed to implement procedures to regularly review records of information system activity, such as audit logs, access reports, and Security Incident tracking reports in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D).

e. MIE failed to implement policies and procedures that, based upon its access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process that includes ePHI in accordance with 45 C.F.R. § 164.308(a)(4)(ii)(C).

f. MIE failed to implement policies and procedures to address Security Incidents, including suspected Security Incidents, to mitigate, to the extent practicable, harmful effects of security incidents known to MIE, or to document such Incidents and their outcomes in accordance with the implementation specifications of the Security Rule, 45 C.F.R. § 164.308(a)(6)(ii).

g. MIE failed to assign a unique name and/or number for identifying and tracking user identity in accordance with the implementation specifications of the Security Rule. 45 C.F.R. § 164.312(a)(2)(i).

h. MIE failed to implement a mechanism to encrypt and decrypt ePHI, in accordance with the implementation specifications of the Security Rule. 45 C.F.R. § 164.312(a)(2)(iv).

i. MIE failed to implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI, in violation of 45 C.F.R. § 164.312(b).

j. MIE failed to implement procedures to verify that a person or entity seeking access to ePHI is the one claimed, in violation of 45 C.F.R. § 164.312(c)(2)(d).

k. MIE failed to adhere to the Minimum Necessary Standard when using or disclosing ePHI, in violation of 45 C.F.R. § 164.502(b)(1).

134. Plaintiff, Kentucky, is entitled to certain statutory damages pursuant to 42 U.S.C. 1320d-5(d)(2).

Count XXII
Kentucky: Deceptive Acts in Violation of Ky. Rev. Stat. § 367.170

135. Plaintiff, Kentucky, incorporates the factual allegations in paragraphs 1 through 44 of this Complaint.

136. The Defendants' conduct constitutes a violation of Ky. Rev. Stat. § 367.170.

137. The information security failings outlined in paragraphs 23 through 43 constitute unfair or deceptive acts in violation of Ky. Rev. Stat. § 367.170.

138. MIE committed an unfair or deceptive act by representing that it maintained appropriate Administrative and Technical Safeguards to protect patients' ePHI, and other appropriate measures to protect consumers' sensitive information, when such was not the case, in violation of Ky. Rev. Stat. § 367.170.

139. Plaintiff, Kentucky, is entitled to civil penalties pursuant to Ky. Rev. Stat. § 367.990(2), and injunctive relief pursuant to Ky. Rev. Stat. § 367.190.

Count XXIII
Louisiana: Violation of HIPAA Safeguards

140. Plaintiff, Louisiana, incorporates the factual allegations in paragraphs 1 through 44 of this Complaint.

141. Defendants' conduct constitutes violations of Administrative Safeguards, Technical Safeguards, and implementation specifications as required by HIPAA. Specifically:

a. MIE failed to review and modify security measures needed to continue the provision of reasonable and appropriate protection of ePHI in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.306(e).

b. MIE failed to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI that it maintained in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(A).

c. MIE failed to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(B).

d. MIE failed to implement procedures to regularly review records of information system activity, such as audit logs, access reports, and Security Incident tracking reports in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D).

e. MIE failed to implement policies and procedures that, based upon its access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process that includes ePHI in accordance with 45 C.F.R. § 164.308(a)(4)(ii)(C).

f. MIE failed to implement policies and procedures to address Security Incidents, including suspected Security Incidents, to mitigate, to the extent practicable, harmful effects of security incidents known to MIE, or to document such Incidents and their outcomes in accordance with the implementation specifications of the Security Rule, 45 C.F.R. § 164.308(a)(6)(ii).

g. MIE failed to assign a unique name and/or number for identifying and tracking user identity in accordance with the implementation specifications of the Security Rule. 45 C.F.R. § 164.312(a)(2)(i).

h. MIE failed to implement a mechanism to encrypt and decrypt ePHI, in accordance with the implementation specifications of the Security Rule. 45 C.F.R. § 164.312(a)(2)(iv).

i. MIE failed to implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI, in violation of 45 C.F.R. § 164.312(b).

j. MIE failed to implement procedures to verify that a person or entity seeking access to ePHI is the one claimed, in violation of 45 C.F.R. § 164.312(c)(2)(d).

k. MIE failed to adhere to the Minimum Necessary Standard when using or disclosing ePHI, in violation of 45 C.F.R. § 164.502(b)(1).

142. Plaintiff, Louisiana, is entitled to certain statutory damages pursuant to 42 U.S.C. 1320d-5(d)(2).

Count XXIV
Louisiana: Deceptive Acts in Violation of La. Rev. Stat. § 51:1405

143. Plaintiff, Louisiana, incorporates the factual allegations in paragraphs 1 through 44 of this Complaint.

144. The Defendants' conduct constitutes a violation of La. Rev. Stat. § 51:1405.

145. The information security failings outlined in paragraphs 30 through 40 constitute unfair or deceptive acts in violation of La. Rev. Stat. § 51:1405.

146. MIE committed an unfair or deceptive act by representing that it maintained appropriate Administrative and Technical Safeguards to protect patients' ePHI, and other appropriate measures to protect consumers' sensitive information, when such was not the case, in violation of La. Rev. Stat. § 51:1405.

147. Plaintiff, Louisiana, is entitled to civil penalties pursuant and injunctive relief pursuant to La. Rev. Stat. § 51:1407.

Count XXV
Louisiana: Data Breach Violation of La. Rev. Stat. § 51:3074

148. Plaintiff, Louisiana, incorporates the factual allegations in paragraphs 1 through 44 of this Complaint.

149. MIE failed to notify affected individuals or others of the Data Breach as required by La. Rev. Stat. § 51:3074.

150. As alleged in paragraphs 28 and 29, Defendants began notifying affected individuals on July 17, 2015 and did not conclude until December 2015. The effective notice date range after the breach was discovered was between 52 days and six months.

151. By waiting between 52 days and six months to notify affected individuals, Defendants violated La. Rev. Stat. § 51:3074.

152. Plaintiff, Louisiana, is entitled to damages and civil penalties pursuant to La. Rev. Stat. 51:3075 and 16 La. Admin. Code Pt III, 701.

Count XXVI
Minnesota: Violation of HIPAA Safeguards

153. Plaintiff, Minnesota, incorporates the factual allegations in paragraphs 1 through 44 of this Complaint.

154. Defendants' conduct constitutes violations of Administrative Safeguards, Technical Safeguards, and implementation specifications as required by HIPAA. Specifically:

a. MIE failed to review and modify security measures needed to continue the provision of reasonable and appropriate protection of ePHI in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.306(e).

b. MIE failed to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI that it maintained in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(A).

c. MIE failed to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(B).

d. MIE failed to implement procedures to regularly review records of information system activity, such as audit logs, access reports, and Security Incident tracking reports in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D).

e. MIE failed to implement policies and procedures that, based upon its access authorization policies, establish, document, review, and modify a user's right of

access to a workstation, transaction, program, or process that includes ePHI in accordance with 45 C.F.R. § 164.308(a)(4)(ii)(C).

f. MIE failed to implement policies and procedures to address Security Incidents, including suspected Security Incidents, to mitigate, to the extent practicable, harmful effects of security incidents known to MIE, or to document such Incidents and their outcomes in accordance with the implementation specifications of the Security Rule, 45 C.F.R. § 164.308(a)(6)(ii).

g. MIE failed to assign a unique name and/or number for identifying and tracking user identity in accordance with the implementation specifications of the Security Rule. 45 C.F.R. § 164.312(a)(2)(i).

h. MIE failed to implement a mechanism to encrypt and decrypt ePHI, in accordance with the implementation specifications of the Security Rule. 45 C.F.R. § 164.312(a)(2)(iv).

i. MIE failed to implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI, in violation of 45 C.F.R. § 164.312(b).

j. MIE failed to implement procedures to verify that a person or entity seeking access to ePHI is the one claimed, in violation of 45 C.F.R. § 164.312(c)(2)(d).

k. MIE failed to adhere to the Minimum Necessary Standard when using or disclosing ePHI, in violation of 45 C.F.R. § 164.502(b)(1).

155. Plaintiff, Minnesota, is entitled to certain statutory damages pursuant to 42 U.S.C. 1320d-5(d)(2).

Count XXVII
Minnesota: Deceptive Acts in Violation of Minn. Stat. § 325F.69

156. Plaintiff, Minnesota, incorporates the factual allegations in paragraphs 1 through 44 of this Complaint.

157. Minnesota Statutes section 325F.69, subdivision 1 reads:

> The act, use, or employment by any person of any fraud, false pretense, false promise, misrepresentation, misleading statement or deceptive practice, with the intent that others rely thereon in connection with the sale of any merchandise, whether or not any person has in fact been misled, deceived, or damaged thereby, is enjoinable as provided in section 325F.70

Minn. Stat. § 325F.69, subd. 1 (2017).

158. The term "merchandise" within the meaning of Minnesota Statutes section 325F.69 includes services. *See* Minn. Stat. § 325F.68, subd. 2 (2017).

159. Defendants have repeatedly violated Minnesota Statutes section 325F.69, subdivision 1, by engaging in the deceptive and fraudulent practices described in this Complaint. For example, Defendants falsely represented to Minnesota persons that Defendants would protect and safeguard their protected health information and sensitive personal information—including, but not limited to, by using encryption tools and maintaining appropriate Administrative and Technical Safeguards to protect Minnesota persons' ePHI, as well as other appropriate measures to protect Minnesota persons' sensitive personal information—when such was not the case, resulting in the exposure of Minnesota persons' protected health information and sensitive personal information as described in this Complaint.

160. As a result of the practices described in this Complaint, hackers accessed and exfiltrated the protected health information of more than 8,000 Minnesotans (including more than 5,000 Minnesotans who also had their Social Security numbers exposed as well). The

protected health information and sensitive personal information that was hacked includes an individual's name, telephone number, mailing address, username, hashed password, security question and answer, spousal information (including name and date of birth), email address, date of birth, Social Security number, lab results, health insurance policy information, diagnosis, disability code, doctor's name, medical conditions, and child's name and birth statistics. These Minnesota persons had their protected health information and personal information exposed in connection with their seeking treatment from healthcare providers, physician practices, hospitals, and/or other organizations which are or were located and/or operated within Minnesota.

161. Special circumstances exist that triggered a duty on the part of Defendants to disclose material facts related to vulnerabilities within Defendants' computer systems to Minnesota persons. First, Defendants had special knowledge of the vulnerabilities in Defendants' computers systems, and that hackers had exposed these vulnerabilities, leading to the release of Minnesotans protected health information and personal information. Minnesotans did not have knowledge of these vulnerabilities or the release of this information at the time of their treatment. Minnesotans lack of knowledge was also caused, in part, by Defendants failure to timely notify Minnesotans of the security breach of Defendants' computer systems. Second, Defendants did not say enough to prevent the representations it made to Minnesotans from being deceptive and misleading.

162. Defendants knew or had reason to know that Minnesotans would place their trust in Defendants and rely on Defendants to inform them of material facts relating to the vulnerabilities in Defendants' computers systems, and that hackers had exposed these vulnerabilities. Defendants abused that trust by making misrepresentations, or concealing material facts, about these vulnerabilities.

163. Given the representations it made, its special knowledge, and the circumstances described in this Complaint, Defendants had a duty to disclose material facts to Minnesota persons in connection with the data breach described in this Complaint. By not doing so, Defendants failed to disclose material information in violation of Minnesota Statutes section 325F.69, subdivision 1.

164. Due to the deceptive and fraudulent conduct described in this Complaint, Minnesota persons made payments to Defendants for goods and services that they otherwise would not have purchased or in amounts that they should not have been required to pay.

165. Defendants' conduct, practices, actions, and material omissions described in this Complaint constitute multiple, separate violations of Minnesota Statutes section 325F.69.

166. Plaintiff, Minnesota, is entitled to civil penalties pursuant to Minn. Stat. § 8.31; attorney fees and costs pursuant to Minn. Stat. § 8.31; injunctive relief pursuant to Minn. Stat. § 8.31 and § 325F.70; restitution under the *parens patriae* doctrine, the general equitable powers of this Court, and§ 8.31; and any such further relief as provided by law or equity, or as the Court deems appropriate and just.

Count XXVIII
Minnesota: Deceptive Acts in Violation of Minn. Stat. § 325D.44

167. Plaintiff, Minnesota, incorporates the factual allegations in paragraphs 1 through 44 of this Complaint.

168. Minnesota Statutes section 325D.44, subdivision 1 provides in part that:

> A person engages in a deceptive trade practice when, in the course of business, vocation, or occupation, the person:
> ***
> (5) represents that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities that they do not have or that a person has a sponsorship, approval, status, affiliation or connection that the person does not have;

> ***
> (7) represents that goods or services are of a particular standard, quality, or grade, or that goods are of a particular style or model, if they are of another;
> *** or
> (13) engages in any other conduct which similarly creates a likelihood of confusion or of misunderstanding.

Minn. Stat. § 325D.44, subd. 1 (2017).

169. Defendants have repeatedly violated Minnesota Statutes section 325D.44, subdivision 1, by engaging in the deceptive and fraudulent conduct described in this Complaint, including by making false, deceptive, fraudulent, and/or misleading representations and material omissions to Minnesota persons regarding their products and services. These misrepresentations and material omissions include but are not limited to: (1) by making misrepresentations about protecting Minnesota persons ePHI and sensitive personal information, Defendants represented that their products and/or services had characteristics that they did not have in violation of Minn. Stat. § 325D.44, subd. 1(5), and were of a particular standard, quality, or grade, when they were of another in violation of Minn. Stat. § 325D.44, subd. 1(7); and (2) by falsely representing to Minnesota persons that Defendants would protect and safeguard their protected health information and sensitive personal information—including, but not limited to, by using encryption tools and maintaining appropriate Administrative and Technical Safeguards to protect Minnesota persons' ePHI, as well as other appropriate measures to protect Minnesota persons' sensitive personal information—when such was not the case, resulting in the exposure of Minnesota persons' protected health information and sensitive personal information as described in this Complaint, Defendant engaged in conduct that creates a likelihood of confusing or of misunderstanding in violation of Minn. Stat. § 325D.44, subd. 1(13).

170. As a result of the practices described in this Complaint, hackers accessed and exfiltrated the protected health information of more than 8,000 Minnesotans (including more than 5,000 Minnesotans who also had their Social Security numbers exposed as well). The protected health information and sensitive personal information that was hacked includes an individual's name, telephone number, mailing address, username, hashed password, security question and answer, spousal information (including name and date of birth), email address, date of birth, Social Security number, lab results, health insurance policy information, diagnosis, disability code, doctor's name, medical conditions, and child's name and birth statistics. These Minnesota persons had their protected health information and personal information exposed as a result of their seeking treatment from healthcare providers, physician practices, hospitals, and/or other organizations which are or were located and/or operated within Minnesota.

171. Special circumstances exist that triggered a duty on the part of Defendants to disclose material facts related to vulnerabilities within Defendants' computer systems to Minnesota persons. First, Defendants had special knowledge of the vulnerabilities in Defendants' computers systems, and that hackers had exposed these vulnerabilities, leading to the release of Minnesotans protected health information and personal information. Minnesota did not have knowledge of these vulnerabilities or the release of this information at the time of their treatment. Minnesotans lack of knowledge was also caused, in part, by Defendants failure to timely notify Minnesotans of the security breach of Defendants' computer systems. Second, Defendants did not say enough to prevent the representations it made to Minnesotans from being deceptive and misleading.

172. Defendants knew or had reason to know that Minnesotans would place their trust in Defendants and rely on Defendants to inform them of material facts relating to the

vulnerabilities in Defendants' computers systems, and that hackers had exposed these vulnerabilities. Defendants abused that trust by making misrepresentations, or concealing material facts, about these vulnerabilities.

173. Given the representations it made, its special knowledge, and the circumstances described in this Complaint, Defendants had a duty to disclose material facts to Minnesota persons in connection with the data breach described in this Complaint. By not doing so, Defendants failed to disclose material information in violation of Minnesota Statutes section 325F.69, subdivision 1.

174. Due to the deceptive and fraudulent conduct described in this Complaint, Minnesota persons made payments to Defendants for goods and services that they otherwise would not have purchased or in amounts that they should not have been required to pay.

175. Defendants' conduct, practices, and actions described in this Complaint constitute multiple, separate violations of Minnesota Statutes section 325D.44.

176. Plaintiff, Minnesota, is entitled to civil penalties pursuant to Minn. Stat. § 8.31; attorney fees and costs pursuant to Minn. Stat. § 8.31; injunctive relief pursuant to Minn. Stat. § 8.31 and § 325D.45; restitution under the *parens patriae* doctrine, the general equitable powers of this Court, and§ 8.31; and any such further relief as provided by law or equity, or as the Court deems appropriate and just.

Count XXIX
Minnesota: Data Breach Violation of Minn. Stat. § 325E.61

177. Plaintiff, Minnesota, incorporates the factual allegations in paragraphs 1 through 44 of this Complaint.

178. MIE failed to notify affected individuals or others of the Data Breach as required by Minn. Stat. § 325E.61.

179. As alleged in paragraphs 28 and 29, Defendants began notifying affected individuals on July 17, 2015 and did not conclude until December 2015. The effective notice date range after the breach was discovered was between 52 days and six months.

180. By waiting between 52 days and six months to notify affected individuals, Defendants violated Minn. Stat. § 325E.61.

181. Minnesota Statutes 325E.61, subdivision 1(a) provides in part that:

> Any person or business that conducts business in this state, and that owns or licenses data that includes personal information, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of this state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure must be made in the most expedient time possible and without unreasonable delay.

Minn. Stat. § 325E.61, subd. 1(a) (2017).

182. At all relevant times, Defendants conducted business in Minnesota and owned or licensed data that included personal information.

183. Defendants have violated Minnesota Statutes section 325E.61, subdivision 1(a) by failing to, without unreasonable delay, expediently notify Minnesota victims of the data breach described in this Complaint. Despite knowing that it exposed the personal information, including persons' names and Social Security numbers, of Minnesota persons, Defendants unreasonably delayed providing notice of this breach to Minnesota residents.

184. Defendants' conduct, practices, and actions described in this Complaint constitute multiple, separate violations of Minnesota Statutes section 325E.61.

185. Plaintiff, Minnesota, is entitled to civil penalties pursuant to Minn. Stat. § 8.31 and § 325E.61, subd. 6; attorney fees and costs pursuant to Minn. Stat. § 8.31 and § 325E.61; subd. 6; injunctive relief pursuant to Minn. Stat. § 8.31 and § 325E.61, subd. 6; restitution under

the *parens patriae* doctrine, the general equitable powers of this Court, and Minn. Stat. § 8.31; and any such further relief as provided by law or equity, or as the Court deems appropriate and just.

Count XXX
Nebraska: Violation of HIPAA Safeguards

186. Plaintiff, Nebraska, incorporates the factual allegations in paragraphs 1 through 44 of this Complaint.

187. Defendants' conduct constitutes violations of Administrative Safeguards, Technical Safeguards, and implementation specifications as required by HIPAA. Specifically:

a. MIE failed to review and modify security measures needed to continue the provision of reasonable and appropriate protection of ePHI in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.306(e).

b. MIE failed to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI that it maintained in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(A).

c. MIE failed to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(B).

d. MIE failed to implement procedures to regularly review records of information system activity, such as audit logs, access reports, and Security Incident

tracking reports in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D).

e. MIE failed to implement policies and procedures that, based upon its access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process that includes ePHI in accordance with 45 C.F.R. § 164.308(a)(4)(ii)(C).

f. MIE failed to implement policies and procedures to address Security Incidents, including suspected Security Incidents, to mitigate, to the extent practicable, harmful effects of security incidents known to MIE, or to document such Incidents and their outcomes in accordance with the implementation specifications of the Security Rule, 45 C.F.R. § 164.308(a)(6)(ii).

g. MIE failed to assign a unique name and/or number for identifying and tracking user identity in accordance with the implementation specifications of the Security Rule. 45 C.F.R. § 164.312(a)(2)(i).

h. MIE failed to implement a mechanism to encrypt and decrypt ePHI, in accordance with the implementation specifications of the Security Rule. 45 C.F.R. § 164.312(a)(2)(iv).

i. MIE failed to implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI, in violation of 45 C.F.R. § 164.312(b).

j. MIE failed to implement procedures to verify that a person or entity seeking access to ePHI is the one claimed, in violation of 45 C.F.R. § 164.312(c)(2)(d).

k. MIE failed to adhere to the Minimum Necessary Standard when using or disclosing ePHI, in violation of 45 C.F.R. § 164.502(b)(1).

188. Plaintiff, Nebraska, is entitled to certain statutory damages pursuant to 42 U.S.C. 1320d-5(d)(2).

Count XXXI
Nebraska: Deceptive Acts in Violation of Neb. Rev. Stat. § 59-1602

189. Plaintiff, Nebraska, incorporates the factual allegations in paragraphs 1 through 44 of this Complaint.

190. The Defendants' conduct constitutes a violation of Neb. Rev. Stat. § 59-1602.

191. The information security failings outlined in paragraphs 30 through 40 constitute unfair or deceptive acts in violation of Neb. Rev. Stat. § 59-1602.

192. MIE committed an unfair or deceptive act by representing that it maintained appropriate Administrative and Technical Safeguards to protect patients' ePHI, and other appropriate measures to protect consumers' sensitive information, when such was not the case, in violation of Neb. Rev. Stat. § 59-1602.

193. Plaintiff, Nebraska, is entitled to civil penalties pursuant to Neb. Rev. Stat. § 59-1614, attorney fees and costs pursuant to Neb. Rev. Stat. § 59-1602(1), and injunctive relief pursuant to Neb. Rev. Stat. § 59-1608.

Count XXXII
Nebraska: Data Breach Violation of Neb. Rev. Stat. § 87-803

194. Plaintiff, Nebraska, incorporates the factual allegations in paragraphs 1 through 44 of this Complaint.

195. MIE failed to notify affected individuals or others of the Data Breach as required by Neb. Rev. Stat. § 87-803.

196. As alleged in paragraphs 28 and 29, Defendants began notifying affected individuals on July 17, 2015 and did not conclude until December 2015. The effective notice date range after the breach was discovered was between 52 days and six months.

197. By waiting between 52 days and six months to notify affected individuals, Defendants violated Neb. Rev. Stat. § 87-803.

198. Plaintiff, Nebraska, is entitled to direct economic damages for each affected Nebraska resident pursuant to Neb. Rev. Stat. § 87-806.

Count XXXIII
North Carolina: Violation of HIPAA Safeguards

199. Plaintiff, North Carolina, incorporates the factual allegations in paragraphs 1 through 44 of this Complaint.

200. Defendants' conduct constitutes violations of Administrative Safeguards, Technical Safeguards, and implementation specifications as required by HIPAA. Specifically:

a. MIE failed to review and modify security measures needed to continue the provision of reasonable and appropriate protection of ePHI in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.306(e).

b. MIE failed to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI that it maintained in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(A).

c. MIE failed to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level in accordance with the

implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(B).

d. MIE failed to implement procedures to regularly review records of information system activity, such as audit logs, access reports, and Security Incident tracking reports in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D).

e. MIE failed to implement policies and procedures that, based upon its access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process that includes ePHI in accordance with 45 C.F.R. § 164.308(a)(4)(ii)(C).

f. MIE failed to implement policies and procedures to address Security Incidents, including suspected Security Incidents, to mitigate, to the extent practicable, harmful effects of security incidents known to MIE, or to document such Incidents and their outcomes in accordance with the implementation specifications of the Security Rule, 45 C.F.R. § 164.308(a)(6)(ii).

g. MIE failed to assign a unique name and/or number for identifying and tracking user identity in accordance with the implementation specifications of the Security Rule. 45 C.F.R. § 164.312(a)(2)(i).

h. MIE failed to implement a mechanism to encrypt and decrypt ePHI, in accordance with the implementation specifications of the Security Rule. 45 C.F.R. § 164.312(a)(2)(iv).

i. MIE failed to implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI, in violation of 45 C.F.R. § 164.312(b).

j. MIE failed to implement procedures to verify that a person or entity seeking access to ePHI is the one claimed, in violation of 45 C.F.R. § 164.312(c)(2)(d).

k. MIE failed to adhere to the Minimum Necessary Standard when using or disclosing ePHI, in violation of 45 C.F.R. § 164.502(b)(1).

201. Plaintiff, North Carolina, is entitled to certain statutory damages pursuant to 42 U.S.C. 1320d-5(d)(2).

Count XXXIV
North Carolina: Deceptive Acts in Violation of N.C. Gen. Stat. § 75-1.1

202. Plaintiff, North Carolina, incorporates the factual allegations in paragraphs 1 through 44 of this Complaint.

203. The Defendants' conduct constitutes a violation of N.C. Gen. Stat. § 75-1.1.

204. The information security failings outlined in paragraphs 30 through 40 constitute unfair or deceptive acts in violation of N.C. Gen. Stat. § 75-1.1.

205. MIE committed an unfair or deceptive act by representing that it maintained appropriate Administrative and Technical Safeguards to protect patients' ePHI, and other appropriate measures to protect consumers' sensitive information, when such was not the case, in violation of N.C. Gen. Stat. § 75-1.1.

206. Plaintiff, North Carolina, is entitled to attorney fees and costs, penalties, and injunctive relief pursuant to N.C. Gen. Stat. § 75-1.1, *et seq*.

Count XXXV
North Carolina: Data Breach Violation of N.C. Gen. Stat. § 75-65

207. Plaintiff, North Carolina, incorporates the factual allegations in paragraphs 1 through 44 of this Complaint.

208. MIE failed to notify affected individuals or others of the Data Breach as required by N.C. Gen. Stat. § 75-65.

209. As alleged in paragraphs 28 and 29, Defendants began notifying affected individuals on July 17, 2015 and did not conclude until December 2015. The effective notice date range after the breach was discovered was between 52 days and six months.

210. By waiting between 52 days and six months to notify affected individuals, Defendants violated N.C. Gen. Stat. § 75-65.

211. Plaintiff, North Carolina, is entitled to attorney fees and costs, penalties, and injunctive relief pursuant to N.C. Gen. Stat. § 75-1.1, *et seq*.

Count XXXVI
Wisconsin: Violation of HIPAA Safeguards

212. Plaintiff, Wisconsin, incorporates the factual allegations in paragraphs 1 through 44 of this Complaint.

213. Defendants' conduct constitutes violations of Administrative Safeguards, Technical Safeguards, and implementation specifications as required by HIPAA. Specifically:

a. MIE failed to review and modify security measures needed to continue the provision of reasonable and appropriate protection of ePHI in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.306(e).

b. MIE failed to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI that it maintained in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(A).

c. MIE failed to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(B).

d. MIE failed to implement procedures to regularly review records of information system activity, such as audit logs, access reports, and Security Incident tracking reports in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D).

e. MIE failed to implement policies and procedures that, based upon its access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process that includes ePHI in accordance with 45 C.F.R. § 164.308(a)(4)(ii)(C).

f. MIE failed to implement policies and procedures to address Security Incidents, including suspected Security Incidents, to mitigate, to the extent practicable, harmful effects of security incidents known to MIE, or to document such Incidents and their outcomes in accordance with the implementation specifications of the Security Rule, 45 C.F.R. § 164.308(a)(6)(ii).

g. MIE failed to assign a unique name and/or number for identifying and tracking user identity in accordance with the implementation specifications of the Security Rule. 45 C.F.R. § 164.312(a)(2)(i).

h. MIE failed to implement a mechanism to encrypt and decrypt ePHI, in accordance with the implementation specifications of the Security Rule. 45 C.F.R. § 164.312(a)(2)(iv).

i. MIE failed to implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI, in violation of 45 C.F.R. § 164.312(b).

j. MIE failed to implement procedures to verify that a person or entity seeking access to ePHI is the one claimed, in violation of 45 C.F.R. § 164.312(c)(2)(d).

k. MIE failed to adhere to the Minimum Necessary Standard when using or disclosing ePHI, in violation of 45 C.F.R. § 164.502(b)(1).

214. Plaintiff, Wisconsin, is entitled to certain statutory damages pursuant to 42 U.S.C. 1320d-5(d)(2).

Count XXXVII
Wisconsin: Fraudulent Representations in Violation of Wis. Stat. § 100.20

215. Plaintiff, Wisconsin, incorporates the factual allegations in paragraphs 1 through 44 of this Complaint.

216. The Defendants' conduct constitutes a violation of Wis. Stat. § 100.20.

217. MIE represented that it maintained appropriate Administrative and Technical Safeguards to protect patients' ePHI, and other appropriate measures to protect consumers' sensitive information, when such was not the case, in violation of Wis. Stat. § 100.18.

218. Plaintiff, Wisconsin, is entitled to civil penalties, attorney's fees and costs, and injunctive relief pursuant to Wis. Stat. §§ 100.26 and 93.20.

Count XXXVIII
Wisconsin: Negligent Disclosure of Patient Health Care Records in Violation of Wis. Stat. § 146.84(2)(b)

219. Plaintiff, Wisconsin, incorporates the factual allegations in paragraphs 1 through 44 of this Complaint.

220. The Defendants negligently disclosed confidential information in violation of Wis. Stat. § 146.82.

221. Plaintiff, Wisconsin, is entitled to civil penalties pursuant to Wis. Stat. § 146.84(2)(b).

THIS COURT'S POWER TO GRANT RELIEF

222. Pursuant to 28 U.S.C. § 1367, this Court has supplemental jurisdiction to allow the Plaintiff States to enforce their state laws against Defendants in this Court and to grant such relief as provided under the following state laws including injunctive relief, civil penalties, attorneys' fees, expenses, costs, and such other relief to which the Plaintiff States may be entitled:

State	Deceptive Acts	Data Breach	PIPA
Arizona:	Ariz. Rev. Stat. §§ 44-1528, 44-1534, and 44-1531		
Arkansas:	Ark. Code Ann. § 4-88-113	Ark. Code Ann. § 4-110-108	Ark. Code Ann. § 4-110-108
Florida:	Sections 501.207, 501.2075, and 501.2105, Florida Statutes	Section 501.171(9), Florida Statutes	Section 501.171(9), Florida Statutes

Indiana:	Ind. Code §§ 24-5-0.5-4(C), and 24-5-0.5-4(G)		Ind. Code § 24-4.9-3-3.5(f)
Iowa:	Iowa Code § 714.16	Iowa Code § 715c.2	
Kansas:	Kan. Stat. §§ 50-632, and 50-636	Kan. Stat. § 50-7a02	Kan. Stat. § 50-6139b
Kentucky:	Ky. Rev. Stat. §§ 367.110-.300, and 367.990		
Louisiana:	La. Rev. Stat. § 51:1401 et seq.	La. Rev. Stat. 51:3071 et seq.	
Minnesota:	Minn. Stat. § 8.31	Minn. Stat. § 8.31	
Nebraska:	Neb. Rev. Stat. §§ 59-1602; 59-1608, and 59-1614	Neb. Rev. Stat. § 87-806	
North Carolina	N.C. Gen. Stat. § 75-1.1, *et seq*.	N.C. Gen. Stat. § 75-65	N.C. Gen. Stat. § 75-60, *et seq*.
Wisconsin:	Wis. Stat. §§ 93.20, 100.18, and 100.26		Wis. Stat. § 146.84(2)(b)

PRAYER FOR RELIEF

WHEREFORE, the Plaintiff States respectfully request that the Court:

A. Award Plaintiffs such injunctive relief as outlined in Exhibit A, to be filed concurrently herewith;

B. Award Plaintiffs a financial judgment for restitution and civil penalties as permitted by statute, and;

C. Award Plaintiffs such other relief the Court deems just and proper.

Respectfully Submitted,

Date: _____

Curtis T. Hill Jr.
Attorney General of Indiana
Atty. No. 13999-20

By: */s/ Taylor C. Byrley*
Taylor C. Byrley, Deputy Attorney General
Atty. No. 35177-49

By: */s/ Michael A. Eades*
Michael A. Eades, Deputy Attorney General
Atty. No. 31015-49

By: */s/ Douglas S. Swetnam*
Douglas S. Swetnam, Section Chief
Atty. No. 15860-49

Data Privacy and Identity Theft Unit
Office of the Attorney General
302 West Washington St., 5th Floor
Indianapolis, IN 46204
Tel: (317) 233-3300
Taylor.Byrley@atg.in.gov
Michael.Eades@atg.in.gov
Douglas.Swetnam@atg.in.gov

Attorney General Mark Brnovich

By: */s/* John C. Gray
John C. Gray (Pro Hac Vice)
Assistant Attorney General
Office of Attorney General Mark Brnovich
2005 N. Central Ave.
Phoenix, AZ 85004
Email: John.Gray@azag.gov
Telephone: (602) 542-7753
Attorney for Plaintiff State of Arizona

Attorney General Leslie Rutledge

By: /s/ Peggy Johnson
Peggy Johnson (Pro Hac Vice)
Assistant Attorney General
Office of Attorney General Leslie Rutledge
323 Center St., Suite 200
Little Rock, AR 72201
Email: peggy.johnson@arkansasag.gov
Telephone: (501) 682-8062
Attorney for Plaintiff State of Arkansas

Attorney General Pam Bondi

By: /s/ Diane Oates
Diane Oates (Pro Hac Vice)
Assistant Attorney General
Office of Attorney General Pam Bondi
110 Southeast 6th Street
Fort Lauderdale, FL 33301
Email: Diane.Oates@myfloridalegal.com
Telephone: (954) 712-4603
Attorney for Plaintiff State of Florida

Attorney General Tom Miller

By: /s/ William Pearson
William Pearson (Pro Hac Vice)
Assistant Attorney General
Office of Attorney General Tom Miller
1305 E. Walnut, 2nd Floor
Des Moines, IA 50319
Email: William.Pearson@ag.iowa.gov
Telephone: (515) 281-3731
Attorney for Plaintiff State of Iowa

Attorney General Derek Schmidt

By: /s/ Sarah Dietz
Sarah Dietz (Pro Hac Vice)
Assistant Attorney General
Office of Attorney General Derek Schmidt
120 S.W. 10th Ave., 2nd Floor
Topeka, KS 66612
Email: sarah.dietz@ag.ks.gov
Telephone: (785) 368-6204
Attorney for Plaintiff State of Kansas

Attorney General Andy Beshear

By: /s/ Kevin R. Winstead
Kevin R. Winstead (Pro Hac Vice)
Assistant Attorney General
Office of Attorney General Andy Beshear
1024 Capital Center Drive
Frankfort, KY 40601
Email: Kevin.Winstead@ky.gov
Telephone: (502) 696-5389
Attorney for Plaintiff Commonwealth of Kentucky

Attorney General Jeff Landry

By: /s/ Alberto A. De Puy
Alberto A. De Puy
Assistant Attorney General
Office of Attorney General Jeff Landry
1885 N. Third St.
Baton Rouge, LA 70802
Email: DePuyA@ag.louisiana.gov
Telephone: (225) 326-647

By: /s/ L. Christopher Styron
L. Christopher Styron (Pro Hac Vice)
Assistant Attorney General
Office of Attorney General Jeff Landry
1885 N. Third St.
Baton Rouge, LA 70802
Email: styronl@ag.louisiana.gov
Telephone: (225) 326-6400
Attorneys for Plaintiff State of Louisiana

Attorney General Lori Swanson

By: /s/ Jason T. Pleggenkuhle
Jason T. Pleggenkuhle (Pro Hac Vice)
Assistant Attorney General
Office of Attorney General Lori Swanson
Bremer Tower, Suite 1200
445 Minnesota St.
St. Paul, MN 55101-2130
Email: jason.pleggenkuhle@ag.state.mn.us
Telephone: (651) 757-1147
Attorney for Plaintiff State of Minnesota

Attorney General Doug Peterson

By: /s/ Daniel J. Birdsall
Daniel J. Birdsall (Pro Hac Vice)
Assistant Attorneys General
Office of Attorney General Doug Peterson
2115 State Capitol
PO Box 98920
Lincoln, NE 68509
Email: dan.birdsall@nebraska.gov
Telephone: (402) 471-1279
Attorney for Plaintiff State of Nebraska

Attorney General Josh Stein

By: /s/ Kimberley A. D'arruda
Kimberley A. D'Arruda (Pro Hac Vice)
Special Deputy Attorney General
North Carolina Department of Justice
Office of Attorney General Joshua H. Stein
P.O. Box 629
Raleigh, NC 27602-0629
Email: kdarruda@ncdoj.gov
Telephone: (919) 716-6013
Attorney for Plaintiff State of North Carolina

Attorney General Brad Schimel

By: /s/ Lara Sutherlin
Lara Sutherlin (Pro Hac Vice)
Wisconsin Department of Justice
Office of Attorney General Brad Schimel
17 W. Main St., P.O. Box 7857
Madison, WI 53707-7857
Email: sutherlinla@doj.state.wi.us
Telephone: (608) 267-7163
Attorney for Plaintiff State of Wisconsin

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF INDIANA

The States of Arizona; Arkansas; Florida; Indiana; Iowa; Kansas; Kentucky; Louisiana; Minnesota; Nebraska; North Carolina; and Wisconsin, Plaintiffs; vs. Medical Informatics Engineering, Inc. d/b/a Enterprise Health, LLC and K&L Holdings, and NoMoreClipboard, LLC, Defendants.	Case No.:

CONSENT JUDGMENT AND ORDER

This Consent Judgment and Order ("Consent Judgment" or "Order") is entered into between the Plaintiff, [STATE; "Plaintiff"], and Defendants Medical Informatics Engineering, Inc., and NoMoreClipboard, LLC, including all of their subsidiaries, affiliates, agents, representatives, employees, successors, and assigns (collectively, "Defendants" and, together with the States, the "Parties") in connection with a multistate investigation comprised of the States of Arizona, Arkansas, Florida, Indiana, Iowa, Kansas, Kentucky, Louisiana, Minnesota, Nebraska, North Carolina, and Wisconsin ("Attorneys General" or "States").

This Order resolves the Plaintiff's investigation of events described in the accompanying Complaint regarding Defendants' compliance with the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936, as amended by the Health Information Technology for Economic and Clinical Health Act, Pub. L. No. 111-5, 123 Stat. 226

Exhibit A

("HIPAA"); state Deceptive Trade Practices Acts; state Personal Information Protection Acts; and state Breach Notification Acts as follows:

State	Deceptive Acts	Data Breach
Arizona:	Ariz. Rev. Stat. § 44-1521 et seq.	
Arkansas:	Ark. Code § 4-88-101 *et seq.*	Ark. Code § 4-110-105
Florida:	Chapter 501, Part II, Florida Statutes	Section 501.171, Florida Statutes
Indiana:	Ind. Code §§ 24-5-0.5-4(C), and 24-5-0.5-4(G)	
Iowa:	Iowa Code § 714.16	Iowa Code § 715c.2
Kansas:	Kan. Stat. §§ 50-632, and 50-636	Kan. Stat. § 50-7a02
Kentucky:	Ky. Rev. Stat. §§ 367.110-.300, and 367.990	
Louisiana:	La. Rev. Stat. § 51:1401 et seq.	La. Rev. Stat. 51:3071 et seq.
Minnesota:	Minn. Stat. §§ 325D.43 *et seq.*; Minn. Stat. §§ 325F.68 *et seq.*	Minn. Stat. § 325E.61
Nebraska:	Neb. Rev. Stat. §§ 59-1602; 59-1608, 59-1614, and 87-301	Neb. Rev. Stat. § 87-806
North Carolina	N.C. Gen. Stat. § 75-1.1, *et seq.*	N.C. Gen. Stat. § 75-65
Wisconsin:	Wis. Stat. §§ 93.20, 100.18, and 100.26	Wis. Stat. § 134.98

I. THE PARTIES

1. The Plaintiff is charged with, among other things, enforcement of the Deceptive Trade Practices Act, the Personal Information Protection Act, and the Breach Notification Act. The Plaintiff, pursuant to 42 U.S.C. § 1320d-5(d), may also enforce HIPAA.

2. Defendant Medical Informatics Engineering, Inc. ("MIE") is a domestic corporation with headquarters located at 6302 Constitution Drive, Fort Wayne, Indiana, 46804.

3. Defendant NoMoreClipboard, LLC ("NMC") is a wholly-owned subsidiary of Medical Informatics Engineering, Inc., headquartered at 6312 Constitution Drive, Fort Wayne, Indiana, 46804.

II. JURISDICTION

4. The Court has jurisdiction over the subject matter and over the Parties for the purpose of entering into this Consent Judgment. The Court retains jurisdiction for the purpose of enabling the Parties to apply to the Court at any time for such further orders and relief as may be necessary for the construction, modification, enforcement, execution or satisfaction of this Consent Judgment.

5. At all times relevant to this matter, Defendants were engaged in trade and commerce affecting consumers in the States insofar as Defendants provided electronic health records services to health care providers in the States. Defendants also maintained a website for patients and client health care providers located in the States.

6. Defendants waive any claim of any defect associated with service of the Plaintiff's Complaint and this Consent Judgment and do not require issuance or service of a Summons.

III. FINDINGS

7. The States allege that Defendants Medical Informatics Engineering, Inc. and NoMoreClipboard, LLC, engaged in conduct in violation of HIPAA, the Deceptive Trade Practices Acts, the Personal Information Protection Acts, and the Breach Notification Acts.

8. The Parties have reached an agreement hereby resolving the issues in dispute without the need for further court action. As evidenced by their signatures below, the Parties consent to the entry of this Consent Judgment and its provisions without trial or adjudication of

any issue of fact or law, and without an admission of liability or wrongdoing with regard to this matter.

9. The Court has reviewed the terms of this Consent Judgment and based upon the Parties' agreement and for good cause shown

IT IS HEREBY ORDERED, ADJUDGED AND AGREED AS FOLLOWS:

IV. EFFECTIVE DATE

10. This Consent Judgment shall be effective on the date it is entered by a court of jurisdiction. The Effective Date of this Consent Judgment shall be XXXX.

V. DEFINITIONS

11. "Administrative Safeguards" shall be defined in accordance with 45 C.F.R. § 164.304 and are administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect Electronic Protected Health Information and to manage the conduct of the covered entity's or business associate's workforce in relation to the protection of that information.

12. "Business Associate" shall be defined in accordance with 45 C.F.R. § 160.103 and is a person or entity that provides certain services to or performs functions on behalf of covered entities, or other business associates of covered entities, that require access to Protected Health Information.

13. "Covered Entity" shall be defined in accordance with 45 C.F.R. § 160.103 and is a health care clearinghouse, health plan, or health care provider that transmits health information in electronic form in connection with a transaction for which the U.S. Department of Health and Human Services has adopted standards.

14. "Data Breach" shall mean the data theft from MIE's and NMC's computer system occurring in or about May 2015.

15. "Electronic Protected Health Information" or "ePHI" shall be defined in accordance with 45 C.F.R. § 160.103.

16. "Generic account" shall be defined as an account assigned for a specific role that can be used by unidentified persons or multiple persons Generic account shall not include service accounts.

17. "Minimum Necessary Standard" shall refer to the requirements of the Privacy Rule that, when using or disclosing Protected Health Information or when requesting Protected Health Information from another Covered Entity or Business Associate, a Covered Entity or Business Associate must make reasonable efforts to limit Protected Health Information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request as defined in 45 C.F.R. § 164.502(b) and § 164.514(d).

18. "Privacy Rule" shall refer to the HIPAA Regulations that establish national standards to safeguard individuals' medical records and other Protected Health Information, including ePHI, that is created, received, used, or maintained by a Covered Entity or Business Associate that performs certain services on behalf of the Covered Entity, specifically 45 C.F.R. Part 160 and 45 C.F.R. Part 164, Subparts A and E.

19. "Protected Health Information" or "PHI" shall be defined in accordance with 45 C.F.R. § 160.103.

20. "Security Incident" shall be synonymous with "Intrusion" and shall be defined as the attempted or successful unauthorized access, use, disclosure, modification, or destruction of

information or interference with system operations in an information system in accordance with 45 C.F.R. § 164.304.

21. "Security Rule" shall refer to the HIPAA Regulations that establish national standards to safeguard individuals' Electronic Protected Health Information that is created, received, used, or maintained by a Covered Entity or Business Associate that performs certain services on behalf of the Covered Entity, specifically 45 C.F.R. Part 160 and 45 C.F.R. Part 164, Subparts A and C.

22. "Technical Safeguards" shall be defined in accordance with 45 C.F.R. § 164.304 and means the technology and the policy and procedures for its use that protect Electronic Protected Health Information and control access to it.

VI. FACTUAL BACKGROUND

23. MIE is a third-party provider that licenses a web-based electronic health record application, known as WebChart, to healthcare providers. NMC provides or has provided patient portal and personal health records services to healthcare providers that enable patients to access and manage their electronic health records.

24. At all relevant times, MIE and NMC were Business Associates within the meaning of HIPAA.

25. As Business Associates, Defendants are required to comply with HIPAA's requirements governing the privacy and security of individually identifiable health information, as set forth in the Privacy and Security Rules.

26. Plaintiff's investigation determined that Defendants, as described in the Complaint, engaged in multiple violations of the Deceptive Trade Practices Act, the Personal Information Protection Act, and HIPAA and the regulations promulgated thereunder.

27. Plaintiff incorporates by reference all the assertions in its Complaint as if asserted herein.

VII. INJUNCTIVE PROVISIONS

WHEREFORE, TO PROTECT CONSUMERS AND ENSURE FUTURE COMPLIANCE WITH THE LAW:

28. Defendants shall comply with all Administrative and Technical Safeguards and implementation specifications required by HIPAA.

29. Defendants shall comply with the Deceptive Trade Practices Acts in connection with their collection, maintenance, and safeguarding of consumers' personal and Protected Health Information, and maintain reasonable security policies and procedures to protect such information.

30. Defendants shall comply with the Breach Notification Acts.

31. Defendants shall comply with the Personal Information Protection Acts.

32. Defendants shall not make any representation that has the capacity, tendency, or effect of deceiving or misleading consumers in connection with the safeguarding of ePHI.

33. Defendants shall implement and maintain an information security program that shall be written and shall contain administrative, technical, and physical safeguards appropriate to: (i) the size and complexity of Defendants' operations; (ii) the nature and scope of Defendants' activities; and (iii) the sensitivity of the personal information that Defendants maintain. It shall be the responsibility of the Privacy Officer or other designated individual to maintain, promulgate, and update the policies and procedures necessary to implement the information security program.

34. Defendants shall not employ the use of generic accounts that can be accessed via the Internet.

35. Defendants shall ensure that no generic account on its information system has administrative privileges.

36. Defendants shall require multi-factor authentication to access any portal they manage in connection with their maintenance of ePHI.

37. Defendants shall implement and maintain a Security Incident and Event Monitoring solution to detect and respond to malicious attacks. The Security Incident and Event Monitoring solution may utilize a suite of different solutions and tools to detect and respond to malicious attacks rather than a single solution.

38. Defendants shall implement and maintain reasonable measures to prevent and detect SQL injection attacks that may impact any ePHI they maintain.

39. Defendants shall implement and maintain reasonable measures with respect to the creation of accounts in systems under the administrative control of Defendants with respect to their own employees with access to ePHI to limit and control their creation and ensure that accounts with access to such ePHI are properly monitored. Defendants shall implement and maintain a data loss prevention technology to detect and prevent unauthorized data exfiltration. The data loss prevention technology may utilize a suite of different solutions and tools to detect and prevent unauthorized data exfiltration.

40. Defendants shall require the use of multi-factor authentication by their employees when remotely accessing their system(s) that store or permit access to ePHI.

41. Defendants shall maintain reasonable policies and procedures to ensure that logs of system activity are regularly and actively reviewed and analyzed in as close to real-time as possible.

42. Defendants shall implement and maintain password policies and procedures related to their employees requiring the use of strong, complex passwords, and ensuring the stored passwords are protected from unauthorized access.

43. Defendants shall educate their clients on strong password policies and promote the use of multi-factor authentication by their clients. Defendants shall make the use of multi-factor authentication as well as Single Sign On (SSO) functions available to their clients.

44. Defendants shall implement and maintain appropriate policies and procedures to respond to Security Incidents.

45. Defendants shall, at least annually, train relevant employees regarding their information privacy and security policies, and shall document such training.

46. Defendants shall, within ninety (90) days of the Effective Date of this Consent Judgment, and thereafter annually for a period of five (5) additional years, engage an independent third-party professional who uses procedures and standards generally accepted in the profession to conduct a current, comprehensive, and thorough risk analysis of security risks and vulnerabilities to ePHI that they create, receive, maintain, or transmit, including a review of the actions or deficiencies that are the subject of the Consent Judgment. A professional qualified to conduct such risk analysis must be: (a) an individual qualified as a Certified Information System Security Professional (CISSP) or as a Certified Information Systems Auditor (CISA); or a similarly qualified person or organization; and (b) have at least five (5) years of experience evaluating the effectiveness of computer systems or information system security. Defendants

may utilize an independent third-party vendor with which they already have a contractual relationship to conduct the risk analysis, so long as the contract between the parties provides that the person or persons performing the analysis on behalf of the independent third-party vendor are qualified as a CISSP or CISA. The independent third-party professional conducting the risk analysis shall prepare a formal report ("Security Report") including its findings and recommendations, a copy of which shall be provided to the Indiana Attorney General no later than one hundred eighty (180) days after the Effective Date of this Consent Judgment, which the Indiana Attorney General may share with the States pursuant to paragraph 59. Each year thereafter, a copy of the Security Report shall be provided to the Indiana Attorney General within thirty (30) days of the anniversary of the completion of the first Security Report, until the expiration of the five (5) year period.

47. Within ninety (90) days of their receipt of each Security Report, Defendants shall review and, to the extent necessary, revise their current policies and procedures based on the findings of the Security Report. Within one hundred eighty (180) days of Defendants' receipt of each Security Report, Defendants shall forward to the Indiana Attorney General a description of any action they take, if no action is taken, a detailed description why no action is necessary, in response to each Security Report. The document submitted to the Indiana Attorney General in response to each Security Report shall be titled "MIE Security Action Report," a copy of which may be shared with the States pursuant to paragraph 59.

48. Each Defendant shall designate a Privacy Officer or other official to ensure compliance with this Consent Judgment. The efforts of the Privacy Officer or other designated official in this regard shall be documented in the MIE Security Action Report that is submitted to the Indiana Attorney General and may be shared with the States pursuant to paragraph 59.

[Section VIII and IX subject to settlement discussions]

VIII. PAYMENT TO THE STATES

49. To be determined.

IX. Consumer Relief

a. To be determined.

X. RELEASE

50. Following full payment of the amounts due by Defendants under this Consent Judgment, the Plaintiff shall release and discharge Defendants from all civil claims that the States could have brought under HIPAA, the Deceptive Trade Practices Act, Personal Information Protection Act, and the Breach Notification Act, based on Defendants' conduct as set forth in the Complaint. Nothing contained in this paragraph shall be construed to limit the ability of the States to enforce the obligations that Defendants, their officers, subsidiaries, affiliates, agents, representatives, employees, successors, and assigns, have under this Consent Judgment. Further, nothing in the Consent Judgment shall be construed to create, waive, or limit any private right of action.

51. Notwithstanding any term of this Consent Judgment, any and all of the following forms of liability are specifically reserved and excluded from the release in paragraph 52 as to any entity or person, including Defendants:

a. Any criminal liability that any person or entity, including Defendants, has or may have to the States.

b. Any civil liability or administrative liability that any person or entity, including Defendants, has or may have to the States under any statute, regulation, or rule not expressly covered by the release in paragraph 52 above, including but not

limited to, any and all of the following claims: (i) State or federal antitrust violations; (ii) State or federal securities violations; (iii) State insurance law violations; or (iv) State or federal tax claims.

X. CONSEQUENCES OF NONCOMPLIANCE

52. Defendants represent that they have fully read this Consent Judgment and understand the legal consequences attendant to entering into this Consent Judgment. Defendants understand that any violation of this Consent Judgment may result in any signatory Attorney General seeking all available relief to enforce this Consent Judgment, including an injunction, civil penalties, court and investigative costs, attorneys' fees, restitution, and any other relief provided by the laws of the State or authorized by a court. If Plaintiff is required to file a petition to enforce any provision of this Judgment against one or more Defendants, the particular Defendant(s) involved in such petition agrees to pay all court costs and reasonable attorneys' fees associated with any successful petition to enforce any provision of this Judgment against such Defendant(s).

XI. GENERAL PROVISIONS

53. Any failure of the Plaintiff to exercise any of its rights under this Consent Judgment shall not constitute a waiver of its rights hereunder.

54. Defendants hereby acknowledge that their undersigned representative or representatives are authorized to enter into and execute this Consent Judgment. Defendants are and have been represented by legal counsel and have been advised by their legal counsel of the meaning and legal effect of this Consent Judgment.

55. This Consent Judgment shall bind Defendants and their officers, subsidiaries, affiliates, agents, representatives, employees, successors, future purchasers, acquiring parties, and assigns.

56. Defendants shall deliver a copy of this Consent Judgment to, or otherwise fully apprise, their executive management having decision-making authority with respect to the subject matter of this Consent Judgment within thirty (30) days of the Effective Date.

57. Defendants assert that the Security Report and the MIE Security Action Report required under this Consent Judgment contain confidential commercial information, confidential financial information, and/or trade secrets, and the States who receive the Security Report or MIE Security Action Report, whether from Defendants or another Attorney General, shall, to the extent permitted under the laws of the States, treat each report as confidential and exempt from disclosure under their respective public records laws.

58. The settlement negotiations resulting in this Consent Judgment have been undertaken by Defendants and the States in good faith and for settlement purposes only, and no evidence of negotiations or communications underlying this Consent Judgment shall be offered or received in evidence in any action or proceeding for any purpose.

59. Defendants waive notice and service of process for any necessary filing relating to this Consent Judgment, and the Court retains jurisdiction over this Consent Judgment and the Parties hereto for the purpose of enforcing and modifying this Consent Judgment and for the purpose of granting such additional relief as may be necessary and appropriate. No modification of the terms of this Consent Judgment shall be valid or binding unless made in writing, signed by the Parties, and approved by the Court in which the Consent Judgment is filed, and then only to the extent specifically set forth in such Court's Order. The Parties may agree in writing, through

counsel, to an extension of any time period specified in this Consent Judgment without a court order.

60. Defendants do not object to ex parte submission and presentation of this Consent Judgment by the Plaintiff to the Court, and do not object to the Court's approval of this Consent Judgment and entry of this Consent Judgment by the clerk of the Court.

61. The Parties agree that this Consent Judgment does not constitute an approval by the Plaintiff of any of Defendants' past or future practices, and Defendants shall not make any representation to the contrary.

62. The requirements of the Consent Judgment are in addition to, and not in lieu of, any other requirements of State or federal law. Nothing in this Order shall be construed as relieving Defendants of the obligation to comply with all local, state, and federal laws, regulations, or rules, nor shall any of the provisions of the Consent Judgment be deemed as permission for Defendants to engage in any acts or practices prohibited by such laws, regulations, or rules.

63. This Consent Judgment shall not create a waiver or limit Defendants' legal rights, remedies, or defenses in any other action by the Plaintiff, except an action to enforce the terms of this Consent Judgment or to demonstrate that Defendants were on notice as to the allegations contained herein.

64. This Consent Judgment shall not waive Defendants' right to defend themselves, or make argument in, any other matter, claim, or suit, including, but not limited to, any investigation or litigation relating to the subject matter or terms of the Consent Judgment, except with regard to an action by the Plaintiff to enforce the terms of this Consent Judgment.

65. This Consent Judgment shall not waive, release, or otherwise affect any claims, defenses, or position that Defendants may have in connection with any investigations, claims, or other matters not released in this Consent Judgment.

66. Defendants shall not participate directly or indirectly in any activity to form or proceed as a separate entity or corporation for the purpose of engaging in acts prohibited in this Consent Judgment or for any other purpose which would otherwise circumvent any part of this Consent Judgment.

67. If any clause, provision, or section of this Consent Judgment shall, for any reason, be held illegal, invalid, or unenforceable, such illegality, invalidity, or unenforceability shall not affect any other clause, provision, or section of this Consent Judgment and this Consent Judgment shall be construed and enforced as if such illegal, invalid, or unenforceable clause, section, or other provision had not been contained herein.

68. Unless otherwise prohibited by law, any signatures by the Parties required for entry of this Consent Judgment may be executed in counterparts, each of which shall be deemed an original, but all of which shall be considered one and the same Consent Judgment.

69. To the extent that there are any, Defendants agree to pay all court costs associated with the filing of this Consent Judgment.

XII. NOTICES UNDER THIS CONSENT JUDGMENT

70. Any notices or other documents required to be sent to the Parties pursuant to the Consent Judgment shall be sent by United States Mail, Certified Return Receipt Requested, or other nationally recognized courier service that provides tracking services and identification of the person signing for the documents. The notices and/or documents required to be submitted to:

Douglas S. Swetnam (IN State Bar #15860-49)

Section Chief – Data Privacy & ID Theft Unit
Office of Attorney General Curtis Hill Jr.
302 W. Washington St., 5th Floor
Indianapolis, IN 46204
Email: douglas.swetnam@atg.in.gov
Telephone: (317) 232-6294

Michael A. Eades (IN State Bar #31015-49)
Deputy Attorney General
Office of Attorney General Curtis Hill, Jr.
302 W. Washington St., 5th Floor
Indianapolis, IN 46204
Email: Michael.Eades@atg.in.gov
Telephone: (317) 234-6681

Taylor C. Byrley (IN State Bar #35177-49)
Deputy Attorney General
Office of Attorney General Curtis Hill Jr.
302 W. Washington St., 5th Floor
Indianapolis, IN 46204
Email: Taylor.Byrley@atg.in.gov
Telephone: (317) 234-2235
Attorneys for Plaintiff State of Indiana

John C. Gray (Pro Hac Vice)
Assistant Attorney General
Office of Attorney General Mark Brnovich
2005 N. Central Ave.
Phoenix, AZ 85004
Email: John.Gray@azag.gov
Telephone: (602) 542-7753
Attorney for Plaintiff State of Arizona

Peggy Johnson (Pro Hac Vice)
Assistant Attorney General
Office of Attorney General Leslie Rutledge
323 Center St., Suite 200
Little Rock, AR 72201
Email: peggy.johnson@arkansasag.gov
Telephone: (501) 682-8062
Attorney for Plaintiff State of Arkansas

Diane Oates (Pro Hac Vice)
Assistant Attorney General
Office of Attorney General Pam Bondi

110 Southeast 6th Street
Fort Lauderdale, FL 33301
Email: Diane.Oates@myfloridalegal.com
Telephone: (954) 712-4603
Attorney for Plaintiff State of Florida

William Pearson (Pro Hac Vice)
Assistant Attorney General
Office of Attorney General Tom Miller
1305 E. Walnut, 2nd Floor
Des Moines, IA 50319
Email: William.Pearson@ag.iowa.gov
Telephone: (515) 281-3731
Attorney for Plaintiff State of Iowa

Sarah Dietz (Pro Hac Vice)
Assistant Attorney General
Office of Attorney General Derek Schmidt
120 S.W. 10th Ave., 2nd Floor
Topeka, KS 66612
Email: sarah.dietz@ag.ks.gov
Telephone: (785) 368-6204
Attorney for Plaintiff State of Kansas

Kevin R. Winstead (Pro Hac Vice)
Assistant Attorney General
Office of Attorney General Andy Beshear
1024 Capital Center Drive
Frankfort, KY 40601
Email: Kevin.Winstead@ky.gov
Telephone: (502) 696-5389
Attorney for Plaintiff Commonwealth of Kentucky

Alberto A. De Puy (Pro Hac Vice)
Assistant Attorney General
Office of Attorney General Jeff Landry
1885 N. Third St.
Baton Rouge, LA 70802
Email: DePuyA@ag.louisiana.gov
Telephone: (225) 326-6471

L. Christopher Styron (Pro Hac Vice)
Assistant Attorney General
Office of Attorney General Jeff Landry
1885 N. Third St.

Baton Rouge, LA 70802
Email: styronl@ag.louisiana.gov
Telephone: (225) 326-6400
Attorneys for Plaintiff State of Louisiana

Jason T. Pleggenkuhle (Pro Hac Vice)
Assistant Attorney General
Office of Attorney General Lori Swanson
Bremer Tower, Suite 1200
445 Minnesota St.
St. Paul, MN 55101-2130
Email: jason.pleggenkuhle@ag.state.mn.us
Telephone: (651) 757-1147
Attorney for Plaintiff State of Minnesota

Daniel J. Birdsall (Pro Hac Vice)
Assistant Attorneys General
Office of Attorney General Doug Peterson
2115 State Capitol
PO Box 98920
Lincoln, NE 68509
Email: dan.birdsall@nebraska.gov
Telephone: (402) 471-1279
Attorney for Plaintiff State of Nebraska

Kimberley A. D'Arruda (Pro Hac Vice)
Special Deputy Attorney General
North Carolina Department of Justice
Office of Attorney General Joshua H. Stein
P.O. Box 629
Raleigh, NC 27602-0629
Email: kdarruda@ncdoj.gov
Telephone: (919) 716-6013
Attorney for Plaintiff State of North Carolina
Lara Sutherlin (Pro Hac Vice)
Wisconsin Department of Justice
Office of Attorney General Brad Schimel
17 W. Main St., P.O. Box 7857
Madison, WI 53707-7857
Email: sutherlinla@doj.state.wi.us
Telephone: (608) 267-7163
Attorney for Plaintiff State of Wisconsin

For Medical Informatics Engineering, Inc. and NoMoreClipboard, LLC:

Claudia D. McCarron
Mullen Coughlin LLC
1275 Drummers Lane, Suite 302
Wayne, PA 19087
Email: cmccarron@mullen.law
Telephone: (267) 930-4787

IT IS SO ORDERED, ADJUDGED AND DECREED, on the _____ day of _____, 20___.

_____
[JUDGE]

Distribution:

Claudia D. McCarron
Mullen Coughlin LLC
1275 Drummers Lane, Suite 302
Wayne, PA 19087
Email: cmccarron@mullen.law
Telephone: (267) 930-4787

Douglas S. Swetnam (IN State Bar #15860-49)
Section Chief – Data Privacy & ID Theft Unit
Office of Attorney General Curtis Hill Jr.
302 W. Washington St., 5th Floor
Indianapolis, IN 46204
Email: douglas.swetnam@atg.in.gov
Telephone: (317) 232-6294

Michael A. Eades (IN State Bar #31015-49)
Deputy Attorney General
Office of Attorney General Curtis Hill, Jr.
302 W. Washington St., 5th Floor
Indianapolis, IN 46204
Email: Michael.Eades@atg.in.gov
Telephone: (317) 234-6681

Taylor C. Byrley (IN State Bar #35177-49)
Deputy Attorney General
Office of Attorney General Curtis Hill Jr.
302 W. Washington St., 5th Floor
Indianapolis, IN 46204
Email: Taylor.Byrley@atg.in.gov
Telephone: (317) 234-2235
Attorneys for Plaintiff State of Indiana

John C. Gray (Pro Hac Vice)
Assistant Attorney General
Office of Attorney General Mark Brnovich
2005 N. Central Ave.
Phoenix, AZ 85004
Email: John.Gray@azag.gov
Telephone: (602) 542-7753
Attorney for Plaintiff State of Arizona

Peggy Johnson (Pro Hac Vice)
Assistant Attorney General
Office of Attorney General Leslie Rutledge
323 Center St., Suite 200
Little Rock, AR 72201
Email: peggy.johnson@arkansasag.gov
Telephone: (501) 682-8062
Attorney for Plaintiff State of Arkansas

Diane Oates (Pro Hac Vice)
Assistant Attorney General
Office of Attorney General Pam Bondi
110 Southeast 6th Street
Fort Lauderdale, FL 33301
Email: Diane.Oates@myfloridalegal.com
Telephone: (954) 712-4603
Attorney for Plaintiff State of Florida

William Pearson (Pro Hac Vice)
Assistant Attorney General
Office of Attorney General Tom Miller
1305 E. Walnut, 2nd Floor
Des Moines, IA 50319
Email: William.Pearson@ag.iowa.gov
Telephone: (515) 281-3731
Attorney for Plaintiff State of Iowa

Sarah Dietz (Pro Hac Vice)
Assistant Attorney General
Office of Attorney General Derek Schmidt
120 S.W. 10th Ave., 2nd Floor
Topeka, KS 66612
Email: sarah.dietz@ag.ks.gov
Telephone: (785) 368-6204
Attorney for Plaintiff State of Kansas

Kevin R. Winstead (Pro Hac Vice)
Assistant Attorney General
Office of Attorney General Andy Beshear
1024 Capital Center Drive
Frankfort, KY 40601
Email: Kevin.Winstead@ky.gov
Telephone: (502) 696-5389
Attorney for Plaintiff Commonwealth of Kentucky

Alberto A. De Puy (Pro Hac Vice)
Assistant Attorney General
Office of Attorney General Jeff Landry
1885 N. Third St.
Baton Rouge, LA 70802
Email: DePuyA@ag.louisiana.gov
Telephone: (225) 326-6471

L. Christopher Styron (Pro Hac Vice)
Assistant Attorney General
Office of Attorney General Jeff Landry
1885 N. Third St.
Baton Rouge, LA 70802
Email: styronl@ag.louisiana.gov
Telephone: (225) 326-6400
Attorneys for Plaintiff State of Louisiana

Jason T. Pleggenkuhle (Pro Hac Vice)
Assistant Attorney General
Office of Attorney General Lori Swanson
Bremer Tower, Suite 1200
445 Minnesota St.
St. Paul, MN 55101-2130
Email: jason.pleggenkuhle@ag.state.mn.us
Telephone: (651) 757-1147
Attorney for Plaintiff State of Minnesota

Daniel J. Birdsall (Pro Hac Vice)
Assistant Attorneys General
Office of Attorney General Doug Peterson
2115 State Capitol
PO Box 98920
Lincoln, NE 68509
Email: dan.birdsall@nebraska.gov
Telephone: (402) 471-1279
Attorney for Plaintiff State of Nebraska

Kimberley A. D'Arruda (Pro Hac Vice)
Special Deputy Attorney General
North Carolina Department of Justice
Office of Attorney General Joshua H. Stein
P.O. Box 629
Raleigh, NC 27602-0629
Email: kdarruda@ncdoj.gov
Telephone: (919) 716-6013
Attorney for Plaintiff State of North Carolina

Lara Sutherlin (Pro Hac Vice)
Wisconsin Department of Justice
Office of Attorney General Brad Schimel
17 W. Main St., P.O. Box 7857
Madison, WI 53707-7857
Email: sutherlinla@doj.state.wi.us
Telephone: (608) 267-7163
Attorney for Plaintiff State of Wisconsin

JS 44 (Rev. 07/16)

CcivIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS

State of Indiana, et al.

(b) County of Residence of First Listed Plaintiff Marion
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*

Douglas S. Swetnam, Office of the Attorney General
302 West Washington, IGCS - 5th Floor, Indianapolis, IN 46204
(317) 232-6294

DEFENDANTS

Medical Infromatics Engineering, Inc. d/b/a Enterprise Health, LLC and K&L Holdings, and NoMoreClipboard, LLC

County of Residence of First Listed Defendant Allen
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

Claudia D. McCarron, Mullen Coughlin, LLC
1275 Drummers Lane, Suite 302 Wayne, PA 19087
(267) 930-4787

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ❒ 1 U.S. Government Plaintiff
- ☒ 3 Federal Question *(U.S. Government Not a Party)*
- ❒ 2 U.S. Government Defendant
- ❒ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*

(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	❒ 1	❒ 1	Incorporated *or* Principal Place of Business In This State	❒ 4	❒ 4
Citizen of Another State	❒ 2	❒ 2	Incorporated *and* Principal Place of Business In Another State	❒ 5	❒ 5
Citizen or Subject of a Foreign Country	❒ 3	❒ 3	Foreign Nation	❒ 6	❒ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

CONTRACT
- ❒ 110 Insurance
- ❒ 120 Marine
- ❒ 130 Miller Act
- ❒ 140 Negotiable Instrument
- ❒ 150 Recovery of Overpayment & Enforcement of Judgment
- ❒ 151 Medicare Act
- ❒ 152 Recovery of Defaulted Student Loans (Excludes Veterans)
- ❒ 153 Recovery of Overpayment of Veteran's Benefits
- ❒ 160 Stockholders' Suits
- ❒ 190 Other Contract
- ❒ 195 Contract Product Liability
- ❒ 196 Franchise

REAL PROPERTY
- ❒ 210 Land Condemnation
- ❒ 220 Foreclosure
- ❒ 230 Rent Lease & Ejectment
- ❒ 240 Torts to Land
- ❒ 245 Tort Product Liability
- ❒ 290 All Other Real Property

TORTS

PERSONAL INJURY
- ❒ 310 Airplane
- ❒ 315 Airplane Product Liability
- ❒ 320 Assault, Libel & Slander
- ❒ 330 Federal Employers' Liability
- ❒ 340 Marine
- ❒ 345 Marine Product Liability
- ❒ 350 Motor Vehicle
- ❒ 355 Motor Vehicle Product Liability
- ❒ 360 Other Personal Injury
- ❒ 362 Personal Injury - Medical Malpractice

PERSONAL INJURY
- ❒ 365 Personal Injury - Product Liability
- ❒ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ❒ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ❒ 370 Other Fraud
- ❒ 371 Truth in Lending
- ❒ 380 Other Personal Property Damage
- ❒ 385 Property Damage Product Liability

CIVIL RIGHTS
- ❒ 440 Other Civil Rights
- ❒ 441 Voting
- ❒ 442 Employment
- ❒ 443 Housing/ Accommodations
- ❒ 445 Amer. w/Disabilities - Employment
- ❒ 446 Amer. w/Disabilities - Other
- ❒ 448 Education

PRISONER PETITIONS

Habeas Corpus:
- ❒ 463 Alien Detainee
- ❒ 510 Motions to Vacate Sentence
- ❒ 530 General
- ❒ 535 Death Penalty

Other:
- ❒ 540 Mandamus & Other
- ❒ 550 Civil Rights
- ❒ 555 Prison Condition
- ❒ 560 Civil Detainee - Conditions of Confinement

FORFEITURE/PENALTY
- ❒ 625 Drug Related Seizure of Property 21 USC 881
- ❒ 690 Other

LABOR
- ❒ 710 Fair Labor Standards Act
- ❒ 720 Labor/Management Relations
- ❒ 740 Railway Labor Act
- ❒ 751 Family and Medical Leave Act
- ❒ 790 Other Labor Litigation
- ❒ 791 Employee Retirement Income Security Act

IMMIGRATION
- ❒ 462 Naturalization Application
- ❒ 465 Other Immigration Actions

BANKRUPTCY
- ❒ 422 Appeal 28 USC 158
- ❒ 423 Withdrawal 28 USC 157

PROPERTY RIGHTS
- ❒ 820 Copyrights
- ❒ 830 Patent
- ❒ 840 Trademark

SOCIAL SECURITY
- ❒ 861 HIA (1395ff)
- ❒ 862 Black Lung (923)
- ❒ 863 DIWC/DIWW (405(g))
- ❒ 864 SSID Title XVI
- ❒ 865 RSI (405(g))

FEDERAL TAX SUITS
- ❒ 870 Taxes (U.S. Plaintiff or Defendant)
- ❒ 871 IRS—Third Party 26 USC 7609

OTHER STATUTES
- ❒ 375 False Claims Act
- ❒ 376 Qui Tam (31 USC 3729(a))
- ❒ 400 State Reapportionment
- ❒ 410 Antitrust
- ❒ 430 Banks and Banking
- ❒ 450 Commerce
- ❒ 460 Deportation
- ❒ 470 Racketeer Influenced and Corrupt Organizations
- ❒ 480 Consumer Credit
- ❒ 490 Cable/Sat TV
- ❒ 850 Securities/Commodities/ Exchange
- ☒ 890 Other Statutory Actions
- ❒ 891 Agricultural Acts
- ❒ 893 Environmental Matters
- ❒ 895 Freedom of Information Act
- ❒ 896 Arbitration
- ❒ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ❒ 950 Constitutionality of State Statutes

V. ORIGIN *(Place an "X" in One Box Only)*

☒ 1 Original Proceeding ❒ 2 Removed from State Court ❒ 3 Remanded from Appellate Court ❒ 4 Reinstated or Reopened ❒ 5 Transferred from Another District *(specify)* ❒ 6 Multidistrict Litigation - Transfer ❒ 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing ***(Do not cite jurisdictional statutes unless diversity)***:
45 C.F.R. § 160 et. seq.

Brief description of cause:
Violations of HIPPA and related State law claims

VII. REQUESTED IN COMPLAINT:

❒ CHECK IF THIS IS A **CLASS ACTION** UNDER RULE 23, F.R.Cv.P.

DEMAND $

CHECK YES only if demanded in complaint:
JURY DEMAND: ❒ Yes ❒ No

VIII. RELATED CASE(S) IF ANY

(See instructions):

JUDGE Robert L. Miller Jr. DOCKET NUMBER 3:15-MD-2667

DATE
12/3/2018

SIGNATURE OF ATTORNEY OF RECORD
s/Douglas S. Swetnam

FOR OFFICE USE ONLY

RECEIPT # AMOUNT APPLYING IFP JUDGE MAG. JUDGE

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44

Authority For Civil Cover Sheet

The JS 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

I.(a) **Plaintiffs-Defendants.** Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.

(b) **County of Residence.** For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)

(c) **Attorneys.** Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)".

II. **Jurisdiction.** The basis of jurisdiction is set forth under Rule 8(a), F.R.Cv.P., which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.
United States plaintiff. (1) Jurisdiction based on 28 U.S.C. 1345 and 1348. Suits by agencies and officers of the United States are included here.
United States defendant. (2) When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.
Federal question. (3) This refers to suits under 28 U.S.C. 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.
Diversity of citizenship. (4) This refers to suits under 28 U.S.C. 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below**; NOTE: federal question actions take precedence over diversity cases.**)

III. **Residence (citizenship) of Principal Parties.** This section of the JS 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.

IV. **Nature of Suit.** Place an "X" in the appropriate box. If the nature of suit cannot be determined, be sure the cause of action, in Section VI below, is sufficient to enable the deputy clerk or the statistical clerk(s) in the Administrative Office to determine the nature of suit. If the cause fits more than one nature of suit, select the most definitive.

V. **Origin.** Place an "X" in one of the seven boxes.
Original Proceedings. (1) Cases which originate in the United States district courts.
Removed from State Court. (2) Proceedings initiated in state courts may be removed to the district courts under Title 28 U.S.C., Section 1441. When the petition for removal is granted, check this box.
Remanded from Appellate Court. (3) Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.
Reinstated or Reopened. (4) Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.
Transferred from Another District. (5) For cases transferred under Title 28 U.S.C. Section 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.
Multidistrict Litigation – Transfer. (6) Check this box when a multidistrict case is transferred into the district under authority of Title 28 U.S.C. Section 1407.
Multidistrict Litigation – Direct File. (8) Check this box when a multidistrict case is filed in the same district as the Master MDL docket.
PLEASE NOTE THAT THERE IS NOT AN ORIGIN CODE 7. Origin Code 7 was used for historical records and is no longer relevant due to changes in statue.

VI. **Cause of Action.** Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC 553 Brief Description: Unauthorized reception of cable service

VII. **Requested in Complaint.** Class Action. Place an "X" in this box if you are filing a class action under Rule 23, F.R.Cv.P.
Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction.
Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.

VIII. **Related Cases.** This section of the JS 44 is used to reference related pending cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.

Date and Attorney Signature. Date and sign the civil cover sheet.