

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

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

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

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

21 Michele Lucan (Pro Hac Vice)
22 Assistant Attorney General
23 Office of Attorney General William Tong
110 Sherman Street
24 Hartford, CT 06105
25 Email: michele.lucan@ct.gov
26 Telephone: (860) 808-5440
Attorney for Plaintiff State of Connecticut

1 Patrice Malloy (Pro Hac Vice)
2 Bureau Chief, Multistate and Privacy Bureau
3 Florida Office of the Attorney General
4 110 SE 6th Street
5 Fort Lauderdale, FL 33301
6 (954) 712-4669
7 Patrice.Malloy@myfloridalegal.com

8 Diane Oates (Pro Hac Vice)
9 Assistant Attorney General
10 Florida Office of the Attorney General
11 110 Southeast 6th Street
12 Fort Lauderdale, FL 33301
13 Email: Diane.Oates@myfloridalegal.com
14 Telephone: (954) 712-4603
15 Attorneys for Plaintiff State of Florida

16 William Pearson (Pro Hac Vice)
17 Assistant Attorney General
18 Office of Attorney General Tom Miller
19 1305 E. Walnut, 2nd Floor
20 Des Moines, IA 50319
21 Email: William.Pearson@ag.iowa.gov
22 Telephone: (515) 281-3731
23 Attorney for Plaintiff State of Iowa

24 Sarah Dietz (Pro Hac Vice)
25 Assistant Attorney General
26 Office of Attorney General Derek Schmidt
27 120 S.W. 10th Ave., 2nd Floor
28 Topeka, KS 66612
29 Email: sarah.dietz@ag.ks.gov
30 Telephone: (785) 368-6204
31 Attorney for Plaintiff State of Kansas

32 Kevin R. Winstead (Pro Hac Vice)
33 Assistant Attorney General
34 Office of Attorney General Andy Beshear
35 1024 Capital Center Drive
36 Frankfort, KY 40601
37 Email: Kevin.Winstead@ky.gov
38 Telephone: (502) 696-5389
39 Attorney for Plaintiff Commonwealth of Kentucky

1 Alberto A. De Puy (Pro Hac Vice)
2 Assistant Attorney General
3 Office of Attorney General Jeff Landry
4 1885 N. Third St.
5 Baton Rouge, LA 70802
6 Email: DePuyA@ag.louisiana.gov
7 Telephone: (225) 326-6471

8 L. Christopher Styron (Pro Hac Vice)
9 Assistant Attorney General
10 Office of Attorney General Jeff Landry
11 1885 N. Third St.
12 Baton Rouge, LA 70802
13 Email: styronl@ag.louisiana.gov
14 Telephone: (225) 326-6400
15 Attorneys for Plaintiff State of Louisiana

16 Kathy Fitzgerald (Pro Hac Vice)
17 Assistant Attorney General
18 Department of Attorney General Dana Nessel
19 Corporate Oversight Division
20 525 W. Ottawa St., 5th Floor
21 Lansing, MI 48933
22 Email: fitzgeraldk@michigan.gov
23 Telephone: (517) 335-7632
24 Attorney for Plaintiff State of Michigan

25 Jason T. Pleggenkuhle (Pro Hac Vice)
26 Assistant Attorney General
27 Office of Attorney General Keith Ellison
28 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

29 Daniel J. Birdsall (Pro Hac Vice)
30 Assistant Attorneys General
31 Office of Attorney General Doug Peterson
32 2115 State Capitol
33 PO Box 98920
34 Lincoln, NE 68509
35 Email: dan.birdsall@nebraska.gov
36 Telephone: (402) 471-1279
37 Attorney for Plaintiff State of Nebraska

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

7 Carolyn U. Smith (Pro Hac Vice)
8 Senior Assistant Attorney General
9 Office of the Attorney General and Reporter Herbert H. Slatery III
10 P.O. Box 20207
11 Nashville, TN 37202-0207
12 Email: carolyn.smith@ag.tn.gov
13 Telephone: (615) 532-2578
14 Attorney for Plaintiff State of Tennessee

12 Tanya L. Godfrey (Pro Hac Vice)
13 Assistant Attorney General
14 Office of the West Virginia Attorney General Patrick Morrissey
15 269 Aikens Center
16 Martinsburg, WV 25404
17 Email: tanya.l.godfrey@wvago.gov
18 Telephone: (304) 267-0239
19 Attorney for Plaintiff State of West Virginia

18 R. Duane Harlow (Pro Hac Vice)
19 Assistant Attorney General
20 Director, Consumer Protection and Antitrust Unit
21 Wisconsin Department of Justice
22 Office of Attorney General Josh Kaul
23 17 W. Main St., P.O. Box 7857
24 Madison, WI 53707-7857
25 Email: HarlowRD@doj.state.wi.us
26 Telephone: (608) 266-2950
27 Attorney for Plaintiff State of Wisconsin
28

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

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

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

22 4. This action is brought, in their representative and individual capacities as
23 provided by state and federal law, by the attorneys general of Arizona, Arkansas, Connecticut,
24 Florida, Indiana, Iowa, Kansas, Kentucky, Louisiana, Michigan, Minnesota, Nebraska, North
25 Carolina, Tennessee, West Virginia, and Wisconsin (collectively the "Attorneys General"). The
26 plaintiffs identified in the paragraph are also referred to collectively as the "Plaintiff States."
27
28

1 Statutes (also referred to as “Breach Notification Acts”), and Personal Information Protection
 2 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.
Connecticut:	Conn. Gen. Stat. § 42-110b et seq.	Conn. Gen. Stat. § 36a-701b	Conn. Gen. Stat. § 42-471
Florida:	Chapter 501, Part II, Florida Statutes	Section 501.171, Florida Statutes	Section 501.171, 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.	
Michigan:	Mich. Comp. Laws § 445.901 et seq.	Mich. Comp. Laws § 445.72(13)	
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 87-302	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.
Tennessee:	Tenn. Code Ann. § 47-18-101 et seq.	Tenn. Cod Ann. § 47-18-2107	Tenn. Code Ann. § 47-18-2110
West Virginia:	W.Va. Code §§ 46A-1-101 et seq., 46A-7-108, and 46A-7-111		
Wisconsin:	Wis. Stat. §§ 93.20, 100.18, and 100.26	Wis. Stat. § 134.98	Wis. Stat. §§ 146.82 and 146.84(2)(b)

DEFENDANTS

1
2
3 14. Defendant MIE is a citizen of the State of Indiana. MIE is a corporation that is
4 incorporated in Indiana and has its principal place of business in Indiana at 6302 Constitution
5 Drive, Fort Wayne, IN 46804.

6 15. Defendant NMC is a citizen of the State of Indiana. NMC is a wholly-owned
7 subsidiary of MIE, is organized in Indiana, and has its principal place of business in Indiana at
8 6312 Constitution Drive, Fort Wayne, IN 46804.

9
10 16. Prior to January 6, 2016, MIE also operated under the name of Enterprise Health.
11 Enterprise Health was a division of MIE. On January 6, 2016, MIE formed Enterprise Health,
12 LLC, which shares founders, officers, employees, offices, and servers with MIE and NMC.

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

18
19 **FACTUAL ALLEGATIONS**

20 18. MIE is a third-party provider that licenses a web-based electronic health record
21 application, known as WebChart, to healthcare providers. MIE, through its subsidiary NMC, also
22 provides patient portal and personal health records services to healthcare providers that enable
23
24
25
26
27
28

1 patients to access and manage their electronic health records. Through its WebChart application,
2 MIE provides electronic health services to physicians and medical facilities nationwide.

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

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

7 21. As Business Associates, Defendants are required to comply with the HIPAA
8 federal standards that govern the security of ePHI, including Security Rules. *See* 45 C.F.R. §
9 164.302.

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

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

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

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

22 26. On June 10, 2015, MIE announced a "data security compromise that has affected
23 the security of some personal and protected health information relating to certain clients and
24
25
26
27
28

1 individuals who have used a Medical Informatics Engineering electronic health record.” *Medical*
2 *Informatics Engineering Updates Notice to Individuals of Data Security Compromise*, MIE (July
3 23, 2015), <http://www.mieweb.com/notice>.

4
5 27. On June 20, 2015, NMC announced “a data security compromise that has affected
6 the security of some personal and protected health information relating to individuals who have
7 used a NoMoreClipboard personal health record or patient portal.” *NoMoreClipboard Notice to*
8 *Individuals of a Data Security Compromise*, NoMoreClipboard (July 23, 2015),
9 <https://www.nomoreclipboard.com/notice>.

10
11 28. Defendants admitted that unauthorized access to their network began on May 7,
12 2015, but they did not discover the suspicious activity until May 26, 2015.

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

18
19 30. MIE admitted that the following information was accessed by the hackers: “an
20 individual’s name, telephone number, mailing address, username, hashed password, security
21 question and answer, spousal information (name and potentially date of birth), email address,
22 date of birth, Social Security number, lab results, health insurance policy information, diagnosis,
23 disability code, doctor’s name, medical conditions, and child’s name and birth statistics.” *MIE*
24 *Notice*, <http://www.mieweb.com/notice>.

25
26 31. NMC admitted that the following information was accessed by the hackers: “an
27 individuals’ [sic] name, home address, Social Security number, username, hashed password,
28

1 spousal information (name and potentially date of birth), security question and answer, email
2 address, date of birth, health information, and health insurance policy information.”

3 *NoMoreClipboard Notice*, <https://www.nomoreclipboard.com/notice>.

4
5 32. Defendants began notifying affected individuals by mail on July 17, 2015. This
6 was two months after the initial breach date of May 7, 2015, and over 50 days after the breach
7 discovery date of May 26, 2015.

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

10
11 34. Defendants’ security framework was deficient in several respects. Defendants
12 failed to implement basic industry-accepted data security measures to protect individual’s health
13 information from unauthorized access. Specifically, Defendants set up a generic “tester” account
14 which could be accessed by using a shared password called “tester” and a second account called
15 “testing” with a shared password of “testing”. In addition to being easily guessed, these generic
16 accounts did not require a unique user identification and password in order to gain remote access.
17 In a formal penetration test conducted by Digital Defense in January 2015, these accounts were
18 identified as high risk, yet Defendants continued to employ the use of these accounts and, in fact,
19 acknowledged establishing the generic accounts at the request of one of its’ health care provider
20 clients so that employees did not have to log-in with a unique user identification and password.

21
22 35. Defendants did not have appropriate security safeguards or controls in place to
23 prevent exploitation of vulnerabilities within their system. The “tester” account did not have
24 privileged access but did allow the attacker to submit a continuous string of queries, known as a
25 SQL injection attack, throughout the database as an authorized user. The queries returned error
26
27
28

1 messages that gave the intruder hints as to why the entry was incorrect, providing valuable
2 insight into the database structure.

3 36. The vulnerability to an SQL injection attack was identified as a high risk during a
4 penetration test performed by Digital Defense in 2014. Digital Defense recommended that
5 Defendant “take appropriate measures to implement the use of parameterized queries, or ensure
6 the sanitization of user input.” The steps taken by Defendants to address this vulnerability were
7 insufficient to mitigate SQL vulnerabilities involved in this incident.
8

9 37. The intruder used information gained from the SQL error messages to access the
10 “checkout” account, which had administrative privileges. The “checkout” account was used to
11 access and exfiltrate more than 1.1 million patient records from Defendants’ databases. The SQL
12 error exploit was also used to obtain a second privileged account called “dcarlson”. The
13 “dcarlson” account was used to access and exfiltrate more than 565,000 additional records that
14 were stored in a database containing NMC patient records.
15

16 38. On May 25, 2015, the attacker initiated a second method of attack by inserting
17 malware called a “c99” cell on Defendants’ system. This malware caused a massive number of
18 records to be extracted from Defendants’ databases. The huge document dump slowed down
19 network performance to such an extent that it triggered a network alarm to the system
20 administrator. The system administrator investigated the event and terminated the malware and
21 data exfiltration on May 26, 2015.
22

23 39. Defendant’s post-breach response was inadequate and ineffective. While the c99
24 attack was being investigated, the attacker continued to extract patient records on May 26 and
25 May 28, using the privileged “checkout” credentials acquired through use of the SQL queries.
26 On those two days, a total of 326,000 patient records were accessed.
27
28

1 40. The breach was not successfully contained until May 29, when a security
2 contractor hired by Defendant identified suspicious IP addresses which led the contractor to
3 uncover the principal SQL attack method.
4

5 41. Defendants failed to implement and maintain an active security monitoring and
6 alert system to detect and alert on anomalous conditions such as data exfiltration, abnormal
7 administrator activities, and remote system access by unfamiliar or foreign IP addresses. The
8 significance of the absence of these security tools cannot be overstated, as two of the IP
9 addresses used to access Defendants’ databases originated from Germany. An active security
10 operations system should have identified remote system access by an unfamiliar IP address and
11 alerted a system administrator to investigate.
12

13 42. Defendants’ privacy policy, in effect at the time of the breach, stated: “Medical
14 Informatics Engineering uses encryption and authentication tools (password and user
15 identification) to protect your personal information...[O]ur employees are aware that certain
16 information provided by our customers is confidential and is to be protected.” Yet Defendants
17 failed to encrypt the sensitive personal information and ePHI within MIE’s computer systems, a
18 protection that, had it been employed, would have rendered the data unusable.
19

20 43. Defendants’ information security policies were deficient and poorly documented.
21 For example, the incident response plan provided by Defendants was incomplete. There are
22 several questions posed in the document that indicate it is still in a coordination or draft stage.
23 Indeed, there is no documented evidence or checklist to indicate that Defendants followed their
24
25
26
27
28

1 own incident response plan. Finally, there is no documentation that Defendants conducted
2 HIPAA Security and Awareness training for 2013, 2014, or 2015, prior to the breach.

3 44. Defendants' actions caused harm to members of the Plaintiff States. Specifically,
4 the victims are subject to emotional distress due to their personal information and ePHI being in
5 the hands of unknown and untrusted individuals, in addition to the increased potential for harm
6 that could result from instances of fraud.
7

8 **DEFENDANTS' LAW VIOLATIONS**

9 **Count I**

10 **Arizona: Violation of HIPAA Safeguards**

11 45. Plaintiff, Arizona, incorporates the factual allegations in paragraphs 1 through 44
12 of this Complaint.
13

14 46. Defendants' conduct constitutes violations of Administrative Safeguards,
15 Technical Safeguards, and implementation specifications as required by HIPAA. Specifically:
16

17 a. MIE failed to review and modify security measures needed to continue the
18 provision of reasonable and appropriate protection of ePHI in accordance with the
19 implementation specifications of the Security Rule, in violation of 45 C.F.R. §
20 164.306(e).

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

25 c. MIE failed to implement security measures sufficient to reduce risks and
26 vulnerabilities to a reasonable and appropriate level in accordance with the
27
28

1 implementation specifications of the Security Rule, in violation of 45 C.F.R. §
2 164.308(a)(1)(ii)(B).

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

7
8 e. MIE failed to implement policies and procedures that, based upon its
9 access authorization policies, establish, document, review, and modify a user's right of
10 access to a workstation, transaction, program, or process that includes ePHI in
11 accordance with 45 C.F.R. § 164.308(a)(4)(ii)(C).

12
13 f. MIE failed to implement policies and procedures to address Security
14 Incidents, including suspected Security Incidents, to mitigate, to the extent practicable,
15 harmful effects of security incidents known to MIE, or to document such Incidents and
16 their outcomes in accordance with the implementation specifications of the Security Rule,
17 45 C.F.R. § 164.308(a)(6)(ii).

18
19 g. MIE failed to assign a unique name and/or number for identifying and
20 tracking user identity in accordance with the implementation specifications of the
21 Security Rule. 45 C.F.R. § 164.312(a)(2)(i).

22
23 h. MIE failed to implement a mechanism to encrypt and decrypt ePHI, in
24 accordance with the implementation specifications of the Security Rule. 45 C.F.R. §
25 164.312(a)(2)(iv).

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

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

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

8
9 47. Plaintiff, Arizona, is entitled to certain statutory damages pursuant to 42 U.S.C.
10 1320d-5(d)(2).

11
12 **Count II**
13 **Arizona: Violation of Ariz. Rev. Stat. § 44-1522**

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

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

17 50. The information security failings outlined in the preceding paragraphs constitute
18 unfair or deceptive acts or practices in violation of Ariz. Rev. Stat. § 44-1522.

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

23 52. Defendants' security failings were also likely to cause substantial injury to
24 consumers, including identity theft, and such injury was not reasonably avoidable by the
25 consumers themselves, particularly in light of Defendants' failure to notify consumers in the
26
27
28

1 most expedient manner possible, nor would such injury be outweighed by any countervailing
2 benefits to consumers or competition.

3 53. Defendants' conduct was also willful, as, among other things, they knew or
4 should have known that their unfair or deceptive acts or practices were unlawful.
5

6 54. Plaintiff, Arizona, is entitled to injunctive relief, restitution to all affected persons,
7 and disgorgement of Defendants' profits or revenues obtained by means of its unlawful conduct
8 pursuant to Ariz. Rev. Stat. § 44-1528; civil penalties pursuant to Ariz. Rev. Stat. § 44-1531; and
9 attorney fees and costs pursuant to Ariz. Rev. Stat. § 44-1534.
10

11 **Count III**
Arkansas: Violation of HIPAA Safeguards

12 55. Plaintiff, Arkansas, incorporates the factual allegations in paragraphs 1 through 44
13 of this Complaint.
14

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

17 a. MIE failed to review and modify security measures needed to continue the
18 provision of reasonable and appropriate protection of ePHI in accordance with the
19 implementation specifications of the Security Rule, in violation of 45 C.F.R. §
20 164.306(e).
21

22 b. MIE failed to conduct an accurate and thorough assessment of the
23 potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI
24 that it maintained in accordance with the implementation specifications of the Security
25 Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(A).
26

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

1 implementation specifications of the Security Rule, in violation of 45 C.F.R. §
2 164.308(a)(1)(ii)(B).

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

7
8 e. MIE failed to implement policies and procedures that, based upon its
9 access authorization policies, establish, document, review, and modify a user's right of
10 access to a workstation, transaction, program, or process that includes ePHI in
11 accordance with 45 C.F.R. § 164.308(a)(4)(ii)(C).

12
13 f. MIE failed to implement policies and procedures to address Security
14 Incidents, including suspected Security Incidents, to mitigate, to the extent practicable,
15 harmful effects of security incidents known to MIE, or to document such Incidents and
16 their outcomes in accordance with the implementation specifications of the Security Rule,
17 45 C.F.R. § 164.308(a)(6)(ii).

18
19 g. MIE failed to assign a unique name and/or number for identifying and
20 tracking user identity in accordance with the implementation specifications of the
21 Security Rule. 45 C.F.R. § 164.312(a)(2)(i).

22
23 h. MIE failed to implement a mechanism to encrypt and decrypt ePHI, in
24 accordance with the implementation specifications of the Security Rule. 45 C.F.R. §
25 164.312(a)(2)(iv).

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

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

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

8
9 57. Plaintiff, Arkansas, is entitled to certain statutory damages pursuant to 42 U.S.C.
10 1320d-5(d)(2).

11
12 **Count IV**
13 **Arkansas: Deceptive Acts in Violation of Ark. § 4-88-101**

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

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

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

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

23 62. Plaintiff, Arkansas, is entitled to civil penalties pursuant to Ark. Code § 4-88-
24 113(a)(3), attorney's fees and costs pursuant to Ark. Code § 4-88-113(e), and injunctive relief
25 pursuant to Ark. Code § 4-88-113(a)(1).
26
27
28

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 32 and 33, 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).

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

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

7
8 f. MIE failed to implement policies and procedures to address Security
9 Incidents, including suspected Security Incidents, to mitigate, to the extent practicable,
10 harmful effects of security incidents known to MIE, or to document such Incidents and
11 their outcomes in accordance with the implementation specifications of the Security Rule,
12 45 C.F.R. § 164.308(a)(6)(ii).

13
14 g. MIE failed to assign a unique name and/or number for identifying and
15 tracking user identity in accordance with the implementation specifications of the
16 Security Rule. 45 C.F.R. § 164.312(a)(2)(i).

17
18 h. MIE failed to implement a mechanism to encrypt and decrypt ePHI, in
19 accordance with the implementation specifications of the Security Rule. 45 C.F.R. §
20 164.312(a)(2)(iv).

21
22 i. MIE failed to implement hardware, software, and/or procedural
23 mechanisms that record and examine activity in information systems that contain or use
24 ePHI, in violation of 45 C.F.R. § 164.312(b).

25
26 j. MIE failed to implement procedures to verify that a person or entity
27 seeking access to ePHI is the one claimed, in violation of 45 C.F.R. § 164.312(c)(2)(d).

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

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

5
6 **Count VIII**
7 **Connecticut: Deceptive Acts in Violation of Conn. Gen. Stat. § 42-110b**

8 75. Plaintiff, Connecticut, incorporates factual allegations in paragraphs 1 through 44
9 of this Complaint.

10 76. The Defendants' conduct constitutes a violation of Conn. Gen. Stat. § 42-110b.

11 77. The information security failings outlined in paragraphs 30 through 40 constitute
12 unfair or deceptive acts in violation of Conn. Gen. Stat. § 42-110b.

13 78. MIE committed an unfair or deceptive act by representing that it maintained
14 appropriate Administrative and Technical Safeguards to protect patients' ePHI, and other
15 appropriate measures to protect consumers' sensitive information, when such was not the case, in
16 violation of Conn. Gen. Stat. § 42-110b. That misrepresentation was reasonably interpreted by
17 consumers, affecting their decisions to provide sensitive information to MIE.

18 79. MIE knew or should have known that its acts and practices alleged herein were
19 unfair and deceptive, and were thus willful violations of Conn. Gen. Stat. §42-110b. MIE is
20 therefore liable for civil penalties of up to \$5,000 per willful violation pursuant to General
21 Statutes §42-110o(b).

22 80. Plaintiff, Connecticut, is entitled to civil penalties pursuant to Conn. Gen. Stat. §
23 42-110o, attorney fees and costs pursuant to Conn. Gen. Stat. § 42-110m, and injunctive relief
24 pursuant to Conn. Gen. Stat. § 42-110m.
25
26
27
28

Count IX

Connecticut: Data Breach Violation of Conn. Gen. Stat. § 36a-701b

81. Plaintiff, Connecticut, incorporates factual allegations in paragraphs 1 through 44 of this Complaint.

82. MIE failed to notify affected individuals or others of the Data Breach as required by Conn. Gen. Stat. § 36a-701b.

83. As alleged in paragraphs 32 and 33, 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.

84. By waiting between 52 days and six months to notify affected individuals, Defendants violated Conn. Gen. Stat. § 36a-701b.

85. Pursuant to Conn. Gen. Stat. § 36a-701b(g), a violation of Conn. Gen. Stat. § 36a-701b constitutes an unfair or deceptive trade practice under Conn. Gen. Stat. § 42-110b.

86. MIE knew or should have known that its acts and practices alleged herein were unfair and deceptive, and were thus willful violations of Conn. Gen. Stat. §42-110b. MIE is therefore liable for civil penalties of up to \$5,000 per willful violation pursuant to General Statutes §42-110o(b).

87. Plaintiff, Connecticut, is entitled to attorney fees and costs, and injunctive relief pursuant to Conn. Gen. Stat. §§ 36a-701b(g), 42-110m, and injunctive relief pursuant to Conn. Gen. Stat. §§ 36a-701b(g) and 42-110m.

Count X

Connecticut: Failure to Implement Reasonable Procedures to Protect Personal Information in Violation of Conn. Gen. Stat. § 42-471

88. Plaintiff, Connecticut, incorporates the factual allegations in paragraphs 1 through 44 of this Complaint.

1 89. Defendants failed to implement and maintain reasonable procedures to protect and
2 safeguard the unlawful disclosure of personal information in violation of Conn. Gen. Stat. § 42-
3 471.

4 90. MIE was in possession of Connecticut consumers’ “personal information” as that
5 term is defined in Conn. Gen. Stat. § 42-471(c).
6

7 91. Defendants failed to implement and maintain reasonable procedures to protect and
8 safeguard personal information in violation of Conn. Gen. Stat. § 42-471.

9 92. Plaintiff, Connecticut, is entitled to civil penalties pursuant to Conn. Gen. Stat. §§
10 42-471(e).
11

12 **Count XI**
13 **Florida: Violation of HIPAA Safeguards**

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

16 94. Defendants’ conduct constitutes violations of Administrative Safeguards,
17 Technical Safeguards, and implementation specifications as required by HIPAA. Specifically:

18 a. MIE failed to review and modify security measures needed to continue the
19 provision of reasonable and appropriate protection of ePHI in accordance with the
20 implementation specifications of the Security Rule, in violation of 45 C.F.R. §
21 164.306(e).
22

23 b. MIE failed to conduct an accurate and thorough assessment of the
24 potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI
25 that it maintained in accordance with the implementation specifications of the Security
26 Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(A).
27
28

1 c. MIE failed to implement security measures sufficient to reduce risks and
2 vulnerabilities to a reasonable and appropriate level in accordance with the
3 implementation specifications of the Security Rule, in violation of 45 C.F.R. §
4 164.308(a)(1)(ii)(B).

5
6 d. MIE failed to implement procedures to regularly review records of
7 information system activity, such as audit logs, access reports, and Security Incident
8 tracking reports in accordance with the implementation specifications of the Security
9 Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D).

10
11 e. MIE failed to implement policies and procedures that, based upon its
12 access authorization policies, establish, document, review, and modify a user's right of
13 access to a workstation, transaction, program, or process that includes ePHI in
14 accordance with 45 C.F.R. § 164.308(a)(4)(ii)(C).

15 f. MIE failed to implement policies and procedures to address Security
16 Incidents, including suspected Security Incidents, to mitigate, to the extent practicable,
17 harmful effects of security incidents known to MIE, or to document such Incidents and
18 their outcomes in accordance with the implementation specifications of the Security Rule,
19 45 C.F.R. § 164.308(a)(6)(ii).

20
21 g. MIE failed to assign a unique name and/or number for identifying and
22 tracking user identity in accordance with the implementation specifications of the
23 Security Rule. 45 C.F.R. § 164.312(a)(2)(i).

24
25 h. MIE failed to implement a mechanism to encrypt and decrypt ePHI, in
26 accordance with the implementation specifications of the Security Rule. 45 C.F.R. §
27 164.312(a)(2)(iv).

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

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

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

8
9 95. Plaintiff, Florida, is entitled to certain statutory damages pursuant to 42 U.S.C.
10 1320d-5(d)(2).

11
12 **Count XII**
13 **Florida: Deceptive Acts in Violation of Section 501.204, Florida Statutes**

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

16 97. The Defendants' conduct constitutes a violation of Section 501.204, Florida
17 Statutes.

18 98. The information security failings outlined in paragraphs 34 through 44 constitute
19 unfair or deceptive acts in violation of Section 501.204, Florida Statutes.

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

24 100. Plaintiff, Florida, is entitled to civil penalties pursuant to Section 501.2075,
25 Florida Statutes, attorney fees and costs pursuant to Section 501.2105, Florida Statutes, and
26 injunctive relief pursuant to Section 501.207(b), Florida Statutes.
27
28

1 **Count XIII**

2 **Florida: Data Breach Violation of Section 501.171, Florida Statutes**

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

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

7
8 103. As alleged in paragraphs 32 and 33, Defendants began notifying affected
9 individuals on July 17, 2015 and did not conclude until December 2015. The effective notice
10 date range after the breach was discovered was between 52 days and six months.

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

13
14 105. Plaintiff, Florida, is entitled to civil penalties pursuant to Section 501.171(9),
15 Florida Statutes, attorney fees and costs pursuant to Section 501.171(9), Florida Statutes and
16 injunctive relief pursuant to Section 501.171(9), Florida Statutes.

17 **Count XIV**

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

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

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

25
26 108. The information security failings outlined in paragraphs 34 through 44 constitute
27 unreasonable safeguard procedures in violation of Section 501.171(2), Florida Statutes.

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

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

7
8 f. MIE failed to implement policies and procedures to address Security
9 Incidents, including suspected Security Incidents, to mitigate, to the extent practicable,
10 harmful effects of security incidents known to MIE, or to document such Incidents and
11 their outcomes in accordance with the implementation specifications of the Security Rule,
12 45 C.F.R. § 164.308(a)(6)(ii).

13
14 g. MIE failed to assign a unique name and/or number for identifying and
15 tracking user identity in accordance with the implementation specifications of the
16 Security Rule. 45 C.F.R. § 164.312(a)(2)(i).

17
18 h. MIE failed to implement a mechanism to encrypt and decrypt ePHI, in
19 accordance with the implementation specifications of the Security Rule. 45 C.F.R. §
20 164.312(a)(2)(iv).

21
22 i. MIE failed to implement hardware, software, and/or procedural
23 mechanisms that record and examine activity in information systems that contain or use
24 ePHI, in violation of 45 C.F.R. § 164.312(b).

25
26 j. MIE failed to implement procedures to verify that a person or entity
27 seeking access to ePHI is the one claimed, in violation of 45 C.F.R. § 164.312(c)(2)(d).

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

3 112. Plaintiff, Indiana, is entitled to certain statutory damages pursuant to 42 U.S.C.
4 1320d-5(d)(2).
5

6 **Count XVI**
7 **Indiana: Deceptive Acts in Violation of Ind. Code § 24-5-0.5-3**

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

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

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

13 116. MIE committed an unfair or deceptive act by representing that it maintained
14 appropriate Administrative and Technical Safeguards to protect patients' ePHI, and other
15 appropriate measures to protect consumers' sensitive information, when such was not the case, in
16 violation of Ind. Code § 24-5-0.5-3.
17

18 117. Plaintiff, Indiana, is entitled to civil penalties pursuant to Ind. Code § 24-5-0.5-
19 4(g), attorney fees and costs pursuant to Ind. Code § 24-5-0.5-4(c), and injunctive relief pursuant
20 to Ind. Code § 24-5-0.5-4(c).
21

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

25 118. Plaintiff, Indiana, incorporates the factual allegations in paragraphs 1 through 44
26 of this Complaint.
27
28

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

4 120. The information security failings outlined in paragraphs 30 through 444 constitute
5 unreasonable safeguard procedures in violation of Ind. Code § 24-5-0.5-3.5.

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

8 122. Plaintiff, Indiana, is entitled to civil penalties pursuant to Ind. Code § 24-4.9-3-
9 3.5(f)(2), attorney fees and costs pursuant to Ind. Code § 24-4.9-3-3.5(f)(3), and injunctive relief
10 pursuant to Ind. Code § 24-4.9-3-3.5(f)(1).

11
12
13 **Count XVIII**
14 **Iowa: Violation of HIPAA Safeguards**

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

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

19 a. MIE failed to review and modify security measures needed to continue the
20 provision of reasonable and appropriate protection of ePHI in accordance with the
21 implementation specifications of the Security Rule, in violation of 45 C.F.R. §
22 164.306(e).

23 b. MIE failed to conduct an accurate and thorough assessment of the
24 potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI
25 that it maintained in accordance with the implementation specifications of the Security
26 Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(A).
27
28

1 c. MIE failed to implement security measures sufficient to reduce risks and
2 vulnerabilities to a reasonable and appropriate level in accordance with the
3 implementation specifications of the Security Rule, in violation of 45 C.F.R. §
4 164.308(a)(1)(ii)(B).
5

6 d. MIE failed to implement procedures to regularly review records of
7 information system activity, such as audit logs, access reports, and Security Incident
8 tracking reports in accordance with the implementation specifications of the Security
9 Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D).
10

11 e. MIE failed to implement policies and procedures that, based upon its
12 access authorization policies, establish, document, review, and modify a user's right of
13 access to a workstation, transaction, program, or process that includes ePHI in
14 accordance with 45 C.F.R. § 164.308(a)(4)(ii)(C).
15

16 f. MIE failed to implement policies and procedures to address Security
17 Incidents, including suspected Security Incidents, to mitigate, to the extent practicable,
18 harmful effects of security incidents known to MIE, or to document such Incidents and
19 their outcomes in accordance with the implementation specifications of the Security Rule,
20 45 C.F.R. § 164.308(a)(6)(ii).
21

22 g. MIE failed to assign a unique name and/or number for identifying and
23 tracking user identity in accordance with the implementation specifications of the
24 Security Rule. 45 C.F.R. § 164.312(a)(2)(i).
25

26 h. MIE failed to implement a mechanism to encrypt and decrypt ePHI, in
27 accordance with the implementation specifications of the Security Rule. 45 C.F.R. §
28 164.312(a)(2)(iv).

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

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

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

8
9 125. Plaintiff, Iowa, is entitled to certain statutory damages pursuant to 42 U.S.C.
10 1320d-5(d)(2).

11
12 **Count XIX**
13 **Iowa: Deceptive Acts in Violation of Iowa Code § 714.16**

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

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

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

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

23 130. Plaintiff, Iowa, is entitled to civil penalties pursuant to Iowa Code § 714.16(8),
24 attorney fees and costs pursuant to Iowa Code § 714.16(11), and injunctive relief pursuant to
25 Iowa Code § 714.16(7).
26
27
28

Count XX

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

1
2
3 131. Plaintiff, Iowa, incorporates the factual allegations in paragraphs 1 through 44 of
4 this Complaint.

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

7
8 133. As alleged in paragraphs 32 and 33, Defendants began notifying affected
9 individuals on July 17, 2015 and did not conclude until December 2015. The effective notice
10 date range after the breach was discovered was between 52 days and six months.

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

13
14 135. Plaintiff, Iowa, is entitled to civil penalties pursuant to Iowa Code §§ 715C.2(9),
15 714.16(7), attorney fees and costs pursuant to Iowa Code §§ 715C.2(9), 714.16(7), and
16 injunctive relief pursuant to Iowa Code §§ 715C.2(9), 714.16(7).

Count XXI

Kansas: Violation of HIPAA Safeguards

17
18
19 136. Plaintiff, Kansas, incorporates the factual allegations in paragraphs 1 through 44
20 of this Complaint.

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

- 23
24 a. MIE failed to review and modify security measures needed to continue the
25 provision of reasonable and appropriate protection of ePHI in accordance with the
26 implementation specifications of the Security Rule, in violation of 45 C.F.R. §
27 164.306(e).
28

1 b. MIE failed to conduct an accurate and thorough assessment of the
2 potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI
3 that it maintained in accordance with the implementation specifications of the Security
4 Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(A).
5

6 c. MIE failed to implement security measures sufficient to reduce risks and
7 vulnerabilities to a reasonable and appropriate level in accordance with the
8 implementation specifications of the Security Rule, in violation of 45 C.F.R. §
9 164.308(a)(1)(ii)(B).
10

11 d. MIE failed to implement procedures to regularly review records of
12 information system activity, such as audit logs, access reports, and Security Incident
13 tracking reports in accordance with the implementation specifications of the Security
14 Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D).
15

16 e. MIE failed to implement policies and procedures that, based upon its
17 access authorization policies, establish, document, review, and modify a user's right of
18 access to a workstation, transaction, program, or process that includes ePHI in
19 accordance with 45 C.F.R. § 164.308(a)(4)(ii)(C).
20

21 f. MIE failed to implement policies and procedures to address Security
22 Incidents, including suspected Security Incidents, to mitigate, to the extent practicable,
23 harmful effects of security incidents known to MIE, or to document such Incidents and
24 their outcomes in accordance with the implementation specifications of the Security Rule,
25 45 C.F.R. § 164.308(a)(6)(ii).
26
27
28

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

4 h. MIE failed to implement a mechanism to encrypt and decrypt ePHI, in
5 accordance with the implementation specifications of the Security Rule. 45 C.F.R. §
6 164.312(a)(2)(iv).

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

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

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

14 138. Plaintiff, Kansas, is entitled to certain statutory damages pursuant to 42 U.S.C.
15 1320d-5(d)(2).

16
17
18
19 **Count XXII**

20 **Kansas: Deceptive Acts in Violation of Kan. Stat. § 50-626**

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

23 140. The Defendants' conduct constitutes a violation of Kan. Stat. § 50-626.

24 141. The information security failings outlined in paragraphs 34 through 43 constitute
25 unfair or deceptive acts in violation of Kan. Stat. § 50-626.

26 142. MIE committed an unfair or deceptive act by representing that it maintained
27 appropriate Administrative and Technical Safeguards to protect patients' ePHI, and other
28

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

3 143. Plaintiff, Kansas, is entitled to civil penalties pursuant to Kan. Stat. § 50-636,
4 attorney fees and costs pursuant to Kan. Stat. § 50-632(a)(4), and injunctive relief pursuant to
5 Kan. Stat. § 50-632(a)(2).
6

7 **Count XXIII**
8 **Kansas: Data Breach Violation of Kan. Stat. § 50-7a02**

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

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

13 146. As alleged in paragraphs 32 and 33, Defendants began notifying affected
14 individuals on July 17, 2015 and did not conclude until December 2015. The effective notice
15 date range after the breach was discovered was between 52 days and six months.
16

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

19 148. Plaintiff, Kansas, is entitled to appropriate relief pursuant Kan. Stat. § 50-7a02(g).
20

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

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

26 150. Defendants failed to implement and maintain reasonable procedures to protect and
27 safeguard the unlawful disclosure of personal information in violation of Kan. Stat. § 50-
28 6139b(b)(1).

1 151. The information security failings outlined in paragraphs 34 through 43 constitute
2 unreasonable safeguard procedures in violation of Kan. Stat. § 50-6139b(b)(1).

3 152. Plaintiff, Kansas, is entitled to civil penalties pursuant to Kan. Stat. §§ 50-
4 6139b(d, e), 50-636, attorney fees and costs pursuant to Kan. Stat. §§ 50-6139b(d, e), 50-636(c),
5 and injunctive relief pursuant to Kan. Stat. §§ 50-6139b(d, e), 50-632(a)(2).
6

7 **Count XXV**
8 **Kentucky: Violation of HIPAA Safeguards**

9 153. Plaintiff, Kentucky, incorporates the factual allegations in paragraphs 1 through
10 44 of this Complaint.

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

13 a. MIE failed to review and modify security measures needed to continue the
14 provision of reasonable and appropriate protection of ePHI in accordance with the
15 implementation specifications of the Security Rule, in violation of 45 C.F.R. §
16 164.306(e).
17

18 b. MIE failed to conduct an accurate and thorough assessment of the
19 potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI
20 that it maintained in accordance with the implementation specifications of the Security
21 Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(A).
22

23 c. MIE failed to implement security measures sufficient to reduce risks and
24 vulnerabilities to a reasonable and appropriate level in accordance with the
25 implementation specifications of the Security Rule, in violation of 45 C.F.R. §
26 164.308(a)(1)(ii)(B).
27
28

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

5
6 e. MIE failed to implement policies and procedures that, based upon its
7 access authorization policies, establish, document, review, and modify a user's right of
8 access to a workstation, transaction, program, or process that includes ePHI in
9 accordance with 45 C.F.R. § 164.308(a)(4)(ii)(C).

10
11 f. MIE failed to implement policies and procedures to address Security
12 Incidents, including suspected Security Incidents, to mitigate, to the extent practicable,
13 harmful effects of security incidents known to MIE, or to document such Incidents and
14 their outcomes in accordance with the implementation specifications of the Security Rule,
15 45 C.F.R. § 164.308(a)(6)(ii).

16
17 g. MIE failed to assign a unique name and/or number for identifying and
18 tracking user identity in accordance with the implementation specifications of the
19 Security Rule. 45 C.F.R. § 164.312(a)(2)(i).

20 h. MIE failed to implement a mechanism to encrypt and decrypt ePHI, in
21 accordance with the implementation specifications of the Security Rule. 45 C.F.R. §
22 164.312(a)(2)(iv).

23
24 i. MIE failed to implement hardware, software, and/or procedural
25 mechanisms that record and examine activity in information systems that contain or use
26 ePHI, in violation of 45 C.F.R. § 164.312(b).

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

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

5
6 155. Plaintiff, Kentucky, is entitled to certain statutory damages pursuant to 42 U.S.C.
7 1320d-5(d)(2).

8 **Count XXVI**

9 **Kentucky: Deceptive Acts in Violation of Ky. Rev. Stat. § 367.170**

10 156. Plaintiff, Kentucky, incorporates the factual allegations in paragraphs 1 through
11 44 of this Complaint.

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

13 158. The information security failings outlined in paragraphs 23 through 44 constitute
14 unfair or deceptive acts in violation of Ky. Rev. Stat. § 367.170.

15 159. MIE committed an unfair or deceptive act by representing that it maintained
16 appropriate Administrative and Technical Safeguards to protect patients' ePHI, and other
17 appropriate measures to protect consumers' sensitive information, when such was not the case, in
18 violation of Ky. Rev. Stat. § 367.170.
19
20

21 160. Plaintiff, Kentucky, is entitled to civil penalties pursuant to Ky. Rev. Stat. §
22 367.990(2), and injunctive relief pursuant to Ky. Rev. Stat. § 367.190.

23 **Count XXVII**

24 **Louisiana: Violation of HIPAA Safeguards**

25 161. Plaintiff, Louisiana, incorporates the factual allegations in paragraphs 1 through
26 44 of this Complaint.

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

3 a. MIE failed to review and modify security measures needed to continue the
4 provision of reasonable and appropriate protection of ePHI in accordance with the
5 implementation specifications of the Security Rule, in violation of 45 C.F.R. §
6 164.306(e).

7
8 b. MIE failed to conduct an accurate and thorough assessment of the
9 potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI
10 that it maintained in accordance with the implementation specifications of the Security
11 Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(A).

12
13 c. MIE failed to implement security measures sufficient to reduce risks and
14 vulnerabilities to a reasonable and appropriate level in accordance with the
15 implementation specifications of the Security Rule, in violation of 45 C.F.R. §
16 164.308(a)(1)(ii)(B).

17
18 d. MIE failed to implement procedures to regularly review records of
19 information system activity, such as audit logs, access reports, and Security Incident
20 tracking reports in accordance with the implementation specifications of the Security
21 Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D).

22
23 e. MIE failed to implement policies and procedures that, based upon its
24 access authorization policies, establish, document, review, and modify a user's right of
25 access to a workstation, transaction, program, or process that includes ePHI in
26 accordance with 45 C.F.R. § 164.308(a)(4)(ii)(C).

1 f. MIE failed to implement policies and procedures to address Security
2 Incidents, including suspected Security Incidents, to mitigate, to the extent practicable,
3 harmful effects of security incidents known to MIE, or to document such Incidents and
4 their outcomes in accordance with the implementation specifications of the Security Rule,
5 45 C.F.R. § 164.308(a)(6)(ii).
6

7 g. MIE failed to assign a unique name and/or number for identifying and
8 tracking user identity in accordance with the implementation specifications of the
9 Security Rule. 45 C.F.R. § 164.312(a)(2)(i).
10

11 h. MIE failed to implement a mechanism to encrypt and decrypt ePHI, in
12 accordance with the implementation specifications of the Security Rule. 45 C.F.R. §
13 164.312(a)(2)(iv).
14

15 i. MIE failed to implement hardware, software, and/or procedural
16 mechanisms that record and examine activity in information systems that contain or use
17 ePHI, in violation of 45 C.F.R. § 164.312(b).
18

19 j. MIE failed to implement procedures to verify that a person or entity
20 seeking access to ePHI is the one claimed, in violation of 45 C.F.R. § 164.312(c)(2)(d).
21

22 k. MIE failed to adhere to the Minimum Necessary Standard when using or
23 disclosing ePHI, in violation of 45 C.F.R. § 164.502(b)(1).
24

25 163. Plaintiff, Louisiana, is entitled to certain statutory damages pursuant to 42 U.S.C.
26 1320d-5(d)(2).
27

28 **Count XXVIII**

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

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

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

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

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

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

10
11
12 **Count XXIX**
13 **Louisiana: Data Breach Violation of La. Rev. Stat. § 51:3074**

14 169. Plaintiff, Louisiana, incorporates the factual allegations in paragraphs 1 through
15 44 of this Complaint.

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

18 171. As alleged in paragraphs 32 and 33, Defendants began notifying affected
19 individuals on July 17, 2015 and did not conclude until December 2015. The effective notice
20 date range after the breach was discovered was between 52 days and six months.

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

23 173. Plaintiff, Louisiana, is entitled to damages and civil penalties pursuant to La. Rev.
24 Stat. 51:3075 and 16 La. Admin. Code Pt III, 701.
25
26
27
28

Count XXX
Michigan: Violation of HIPAA Safeguards

1
2
3 174. Plaintiff, Michigan, incorporates the factual allegations in paragraphs 1 through
4 44 of this Complaint.

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

7
8 a. MIE failed to review and modify security measures needed to continue the
9 provision of reasonable and appropriate protection of ePHI in accordance with the
10 implementation specifications of the Security Rule, in violation of 45 C.F.R. §
11 164.306(e).

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

16
17 c. MIE failed to implement security measures sufficient to reduce risks and
18 vulnerabilities to a reasonable and appropriate level in accordance with the
19 implementation specifications of the Security Rule, in violation of 45 C.F.R. §
20 164.308(a)(1)(ii)(B).

21
22 d. MIE failed to implement procedures to regularly review records of
23 information system activity, such as audit logs, access reports, and Security Incident
24 tracking reports in accordance with the implementation specifications of the Security
25 Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D).

26
27 e. MIE failed to implement policies and procedures that, based upon its
28 access authorization policies, establish, document, review, and modify a user's right of

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

3 f. MIE failed to implement policies and procedures to address Security
4 Incidents, including suspected Security Incidents, to mitigate, to the extent practicable,
5 harmful effects of security incidents known to MIE, or to document such Incidents and
6 their outcomes in accordance with the implementation specifications of the Security Rule,
7 45 C.F.R. § 164.308(a)(6)(ii).

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

11 h. MIE failed to implement a mechanism to encrypt and decrypt ePHI, in
12 accordance with the implementation specifications of the Security Rule. 45 C.F.R. §
13 164.312(a)(2)(iv).

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

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

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

21 176. Plaintiff, Michigan, is entitled to certain statutory damages pursuant to 42 U.S.C.
22 1320d-5(d)(2).

Count XXXI

Michigan: Deceptive Acts in Violation of Mich. Comp. Laws § 445.901

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

178. The Defendants' conduct constitutes a violation of Mich. Comp. Laws § 445.901.

179. The information security failings outlined in paragraphs 30 through 43 constitute unfair or deceptive acts in violation of Mich. Comp. Laws § 445.901.

180. 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 Mich. Comp. Laws § 445.901.

181. Plaintiff, Michigan, is entitled to civil penalties pursuant to Mich. Comp. Laws § 445.905, and injunctive relief pursuant to Mich. Comp. Laws § 445.905.

Count XXXII

Michigan: Data Breach Violation of Mich. Comp. Laws § 445.72

182. Plaintiff, Michigan, incorporates the factual allegations in paragraphs 1 through 44 of this Complaint.

183. MIE failed to notify affected individuals or others of the Data Breach as required by Mich. Comp. Laws § 445.72.

184. As alleged in paragraphs 32 and 33, 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.

185. By waiting between 52 days and six months to notify affected individuals, Defendants violated Mich. Comp. Laws § 445.72.

1 186. Plaintiff, Michigan, is entitled to civil penalties pursuant to Mich. Comp. Laws §
2 445.72(13).

3 **Count XXXIII**
4 **Minnesota: Violation of HIPAA Safeguards**

5 187. Plaintiff, Minnesota, incorporates the factual allegations in paragraphs 1 through
6 44 of this Complaint.

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

9 a. MIE failed to review and modify security measures needed to continue the
10 provision of reasonable and appropriate protection of ePHI in accordance with the
11 implementation specifications of the Security Rule, in violation of 45 C.F.R. §
12 164.306(e).

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

17 c. MIE failed to implement security measures sufficient to reduce risks and
18 vulnerabilities to a reasonable and appropriate level in accordance with the
19 implementation specifications of the Security Rule, in violation of 45 C.F.R. §
20 164.308(a)(1)(ii)(B).

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

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

5
6 f. MIE failed to implement policies and procedures to address Security
7 Incidents, including suspected Security Incidents, to mitigate, to the extent practicable,
8 harmful effects of security incidents known to MIE, or to document such Incidents and
9 their outcomes in accordance with the implementation specifications of the Security Rule,
10 45 C.F.R. § 164.308(a)(6)(ii).

11
12 g. MIE failed to assign a unique name and/or number for identifying and
13 tracking user identity in accordance with the implementation specifications of the
14 Security Rule. 45 C.F.R. § 164.312(a)(2)(i).

15
16 h. MIE failed to implement a mechanism to encrypt and decrypt ePHI, in
17 accordance with the implementation specifications of the Security Rule. 45 C.F.R. §
18 164.312(a)(2)(iv).

19
20 i. MIE failed to implement hardware, software, and/or procedural
21 mechanisms that record and examine activity in information systems that contain or use
22 ePHI, in violation of 45 C.F.R. § 164.312(b).

23
24 j. MIE failed to implement procedures to verify that a person or entity
25 seeking access to ePHI is the one claimed, in violation of 45 C.F.R. § 164.312(c)(2)(d).

26
27 k. MIE failed to adhere to the Minimum Necessary Standard when using or
28 disclosing ePHI, in violation of 45 C.F.R. § 164.502(b)(1).

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

3
4 **Count XXXIV**
5 **Minnesota: Deceptive Acts in Violation of Minn. Stat. § 325F.69**

6 190. Plaintiff, Minnesota, incorporates the factual allegations in paragraphs 1 through
7 44 of this Complaint.

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

9 The act, use, or employment by any person of any fraud, false
10 pretense, false promise, misrepresentation, misleading statement or
11 deceptive practice, with the intent that others rely thereon in
12 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

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

14 192. The term “merchandise” within the meaning of Minnesota Statutes section
15 325F.69 includes services. *See* Minn. Stat. § 325F.68, subd. 2 (2017).

16
17 193. Defendants have repeatedly violated Minnesota Statutes section 325F.69,
18 subdivision 1, by engaging in the deceptive and fraudulent practices described in this Complaint.
19 For example, Defendants falsely represented to Minnesota persons that Defendants would protect
20 and safeguard their protected health information and sensitive personal information—including,
21 but not limited to, by using encryption tools and maintaining appropriate Administrative and
22 Technical Safeguards to protect Minnesota persons’ ePHI, as well as other appropriate measures
23 to protect Minnesota persons’ sensitive personal information—when such was not the case,
24 resulting in the exposure of Minnesota persons’ protected health information and sensitive
25 personal information as described in this Complaint.
26
27
28

1 194. As a result of the practices described in this Complaint, hackers accessed and
2 exfiltrated the protected health information of more than 8,000 Minnesotans (including more
3 than 5,000 Minnesotans who also had their Social Security numbers exposed as well). The
4 protected health information and sensitive personal information that was hacked includes an
5 individual's name, telephone number, mailing address, username, hashed password, security
6 question and answer, spousal information (including name and date of birth), email address, date
7 of birth, Social Security number, lab results, health insurance policy information, diagnosis,
8 disability code, doctor's name, medical conditions, and child's name and birth statistics. These
9 Minnesota persons had their protected health information and personal information exposed in
10 connection with their seeking treatment from healthcare providers, physician practices, hospitals,
11 and/or other organizations which are or were located and/or operated within Minnesota.
12
13

14 195. Special circumstances exist that triggered a duty on the part of Defendants to
15 disclose material facts related to vulnerabilities within Defendants' computer systems to
16 Minnesota persons. First, Defendants had special knowledge of the vulnerabilities in Defendants'
17 computers systems, and that hackers had exposed these vulnerabilities, leading to the release of
18 Minnesotans protected health information and personal information. Minnesotans did not have
19 knowledge of these vulnerabilities or the release of this information at the time of their treatment.
20 Minnesotans lack of knowledge was also caused, in part, by Defendants failure to timely notify
21 Minnesotans of the security breach of Defendants' computer systems. Second, Defendants did
22 not say enough to prevent the representations it made to Minnesotans from being deceptive and
23 misleading.
24
25

26 196. Defendants knew or had reason to know that Minnesotans would place their trust
27 in Defendants and rely on Defendants to inform them of material facts relating to the
28

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

4
5 197. Given the representations it made, its special knowledge, and the circumstances
6 described in this Complaint, Defendants had a duty to disclose material facts to Minnesota
7 persons in connection with the data breach described in this Complaint. By not doing so,
8 Defendants failed to disclose material information in violation of Minnesota Statutes section
9 325F.69, subdivision 1.

10
11 198. Due to the deceptive and fraudulent conduct described in this Complaint,
12 Minnesota persons made payments to Defendants for goods and services that they otherwise
13 would not have purchased or in amounts that they should not have been required to pay.

14
15 199. Defendants' conduct, practices, actions, and material omissions described in this
16 Complaint constitute multiple, separate violations of Minnesota Statutes section 325F.69.

17
18 200. Plaintiff, Minnesota, is entitled to civil penalties pursuant to Minn. Stat. § 8.31;
19 attorney fees and costs pursuant to Minn. Stat. § 8.31; injunctive relief pursuant to Minn. Stat.
20 § 8.31 and § 325F.70; restitution under the *parens patriae* doctrine, the general equitable powers
21 of this Court, and § 8.31; and any such further relief as provided by law or equity, or as the Court
22 deems appropriate and just.

23 **Count XXXV**
Minnesota: Deceptive Acts in Violation of Minn. Stat. § 325D.44

24
25 201. Plaintiff, Minnesota, incorporates the factual allegations in paragraphs 1 through
26 44 of this Complaint.

27
28 202. Minnesota Statutes section 325D.44, subdivision 1 provides in part that:

1 A person engages in a deceptive trade practice when, in the course
2 of business, vocation, or occupation, the person:

3 (5) represents that goods or services have sponsorship, approval,
4 characteristics, ingredients, uses, benefits, or quantities that they do
5 not have or that a person has a sponsorship, approval, status,
6 affiliation or connection that the person does not have;

6 (7) represents that goods or services are of a particular standard,
7 quality, or grade, or that goods are of a particular style or model, if
8 they are of another;

*** or

8 (13) engages in any other conduct which similarly creates a
9 likelihood of confusion or of misunderstanding.

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

11 203. Defendants have repeatedly violated Minnesota Statutes section 325D.44,
12 subdivision 1, by engaging in the deceptive and fraudulent conduct described in this Complaint,
13 including by making false, deceptive, fraudulent, and/or misleading representations and material
14 omissions to Minnesota persons regarding their products and services. These misrepresentations
15 and material omissions include but are not limited to: (1) by making misrepresentations about
16 protecting Minnesota persons ePHI and sensitive personal information, Defendants represented
17 that their products and/or services had characteristics that they did not have in violation of Minn.
18 Stat. § 325D.44, subd. 1(5), and were of a particular standard, quality, or grade, when they were
19 of another in violation of Minn. Stat. § 325D.44, subd. 1(7); and (2) by falsely representing to
20 Minnesota persons that Defendants would protect and safeguard their protected health
21 information and sensitive personal information—including, but not limited to, by using
22 encryption tools and maintaining appropriate Administrative and Technical Safeguards to protect
23 Minnesota persons' ePHI, as well as other appropriate measures to protect Minnesota persons'
24 sensitive personal information—when such was not the case, resulting in the exposure of
25 Minnesota persons' protected health information and sensitive personal information as described
26
27
28

1 in this Complaint, Defendant engaged in conduct that creates a likelihood of confusing or of
2 misunderstanding in violation of Minn. Stat. § 325D.44, subd. 1(13).

3 204. As a result of the practices described in this Complaint, hackers accessed and
4 exfiltrated the protected health information of more than 8,000 Minnesotans (including more
5 than 5,000 Minnesotans who also had their Social Security numbers exposed as well). The
6 protected health information and sensitive personal information that was hacked includes an
7 individual's name, telephone number, mailing address, username, hashed password, security
8 question and answer, spousal information (including name and date of birth), email address, date
9 of birth, Social Security number, lab results, health insurance policy information, diagnosis,
10 disability code, doctor's name, medical conditions, and child's name and birth statistics. These
11 Minnesota persons had their protected health information and personal information exposed as a
12 result of their seeking treatment from healthcare providers, physician practices, hospitals, and/or
13 other organizations which are or were located and/or operated within Minnesota.
14

15
16 205. Special circumstances exist that triggered a duty on the part of Defendants to
17 disclose material facts related to vulnerabilities within Defendants' computer systems to
18 Minnesota persons. First, Defendants had special knowledge of the vulnerabilities in Defendants'
19 computers systems, and that hackers had exposed these vulnerabilities, leading to the release of
20 Minnesotans protected health information and personal information. Minnesota did not have
21 knowledge of these vulnerabilities or the release of this information at the time of their treatment.
22 Minnesotans lack of knowledge was also caused, in part, by Defendants failure to timely notify
23 Minnesotans of the security breach of Defendants' computer systems. Second, Defendants did
24 not say enough to prevent the representations it made to Minnesotans from being deceptive and
25 misleading.
26
27
28

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

3 213. As alleged in paragraphs 32 and 33, Defendants began notifying affected
4 individuals on July 17, 2015 and did not conclude until December 2015. The effective notice
5 date range after the breach was discovered was between 52 days and six months.
6

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

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

10
11 Any person or business that conducts business in this state, and that
12 owns or licenses data that includes personal information, shall
13 disclose any breach of the security of the system following
14 discovery or notification of the breach in the security of the data to
15 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.

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

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

19 217. Defendants have violated Minnesota Statutes section 325E.61, subdivision 1(a) by
20 failing to, without unreasonable delay, expediently notify Minnesota victims of the data breach
21 described in this Complaint. Despite knowing that it exposed the personal information, including
22 persons' names and Social Security numbers, of Minnesota persons, Defendants unreasonably
23 delayed providing notice of this breach to Minnesota residents.
24

25 218. Defendants' conduct, practices, and actions described in this Complaint constitute
26 multiple, separate violations of Minnesota Statutes section 325E.61.
27
28

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

5
6 e. MIE failed to implement policies and procedures that, based upon its
7 access authorization policies, establish, document, review, and modify a user's right of
8 access to a workstation, transaction, program, or process that includes ePHI in
9 accordance with 45 C.F.R. § 164.308(a)(4)(ii)(C).

10
11 f. MIE failed to implement policies and procedures to address Security
12 Incidents, including suspected Security Incidents, to mitigate, to the extent practicable,
13 harmful effects of security incidents known to MIE, or to document such Incidents and
14 their outcomes in accordance with the implementation specifications of the Security Rule,
15 45 C.F.R. § 164.308(a)(6)(ii).

16
17 g. MIE failed to assign a unique name and/or number for identifying and
18 tracking user identity in accordance with the implementation specifications of the
19 Security Rule. 45 C.F.R. § 164.312(a)(2)(i).

20 h. MIE failed to implement a mechanism to encrypt and decrypt ePHI, in
21 accordance with the implementation specifications of the Security Rule. 45 C.F.R. §
22 164.312(a)(2)(iv).

23
24 i. MIE failed to implement hardware, software, and/or procedural
25 mechanisms that record and examine activity in information systems that contain or use
26 ePHI, in violation of 45 C.F.R. § 164.312(b).

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

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

5
6 222. Plaintiff, Nebraska, is entitled to certain statutory damages pursuant to 42 U.S.C.
7 1320d-5(d)(2).

8 **Count XXXVIII**

9 **Nebraska: Deceptive Acts in Violation of Neb. Rev. Stat. § 59-1602**

10 223. Plaintiff, Nebraska, incorporates the factual allegations in paragraphs 1 through
11 44 of this Complaint.

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

13 225. The information security failings outlined in paragraphs 34 through 44 constitute
14 unfair or deceptive acts in violation of Neb. Rev. Stat. § 59-1602.

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

19 227. Plaintiff, Nebraska, is entitled to civil penalties pursuant to Neb. Rev. Stat. § 59-
20 1614, attorney fees and costs pursuant to Neb. Rev. Stat. § 59-1602(1), and injunctive relief
21 pursuant to Neb. Rev. Stat. § 59-1608.

22 **Count XXXIX**

23 **Nebraska: Data Breach Violation of Neb. Rev. Stat. § 87-803**

24 228. Plaintiff, Nebraska, incorporates the factual allegations in paragraphs 1 through
25 44 of this Complaint.

1 measures to protect consumers' sensitive information, when such was not the case, in violation
2 of Neb. Rev. Stat. § 87-302(a)(5) and (8).

3 237. Plaintiff, Nebraska, is entitled to civil penalties pursuant to Neb. Rev. Stat. § 87-
4 303.11, attorney fees and costs pursuant to Neb. Rev. Stat. § 87-303(b), and injunctive relief
5 pursuant to Neb. Rev. Stat. § 87-303.05(1).
6

7
8
9 **Count XLI**
10 **North Carolina: Violation of HIPAA Safeguards**

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

13 239. Defendants' conduct constitutes violations of Administrative Safeguards,
14 Technical Safeguards, and implementation specifications as required by HIPAA. Specifically:
15

16 a. MIE failed to review and modify security measures needed to continue the
17 provision of reasonable and appropriate protection of ePHI in accordance with the
18 implementation specifications of the Security Rule, in violation of 45 C.F.R. §
19 164.306(e).
20

21 b. MIE failed to conduct an accurate and thorough assessment of the
22 potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI
23 that it maintained in accordance with the implementation specifications of the Security
24 Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(A).
25

26 c. MIE failed to implement security measures sufficient to reduce risks and
27 vulnerabilities to a reasonable and appropriate level in accordance with the
28

1 implementation specifications of the Security Rule, in violation of 45 C.F.R. §
2 164.308(a)(1)(ii)(B).

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

7
8 e. MIE failed to implement policies and procedures that, based upon its
9 access authorization policies, establish, document, review, and modify a user's right of
10 access to a workstation, transaction, program, or process that includes ePHI in
11 accordance with 45 C.F.R. § 164.308(a)(4)(ii)(C).

12
13 f. MIE failed to implement policies and procedures to address Security
14 Incidents, including suspected Security Incidents, to mitigate, to the extent practicable,
15 harmful effects of security incidents known to MIE, or to document such Incidents and
16 their outcomes in accordance with the implementation specifications of the Security Rule,
17 45 C.F.R. § 164.308(a)(6)(ii).

18
19 g. MIE failed to assign a unique name and/or number for identifying and
20 tracking user identity in accordance with the implementation specifications of the
21 Security Rule. 45 C.F.R. § 164.312(a)(2)(i).

22
23 h. MIE failed to implement a mechanism to encrypt and decrypt ePHI, in
24 accordance with the implementation specifications of the Security Rule. 45 C.F.R. §
25 164.312(a)(2)(iv).

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

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

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

8
9 240. Plaintiff, North Carolina, is entitled to certain statutory damages pursuant to 42
10 U.S.C. 1320d-5(d)(2).

11
12 **Count XLII**
13 **North Carolina: Deceptive Acts in Violation of N.C. Gen. Stat. § 75-1.1**

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

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

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

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

23
24 245. Plaintiff, North Carolina, is entitled to attorney fees and costs, penalties, and
25 injunctive relief pursuant to N.C. Gen. Stat. § 75-1.1, *et seq.*

Count XLIII

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

1
2
3 246. Plaintiff, North Carolina, incorporates the factual allegations in paragraphs 1
4 through 44 of this Complaint.

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

7
8 248. As alleged in paragraphs 32 and 33, Defendants began notifying affected
9 individuals on July 17, 2015 and did not conclude until December 2015. The effective notice
10 date range after the breach was discovered was between 52 days and six months.

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

13
14 250. Plaintiff, North Carolina, is entitled to attorney fees and costs, penalties, and
15 injunctive relief pursuant to N.C. Gen. Stat. § 75-1.1, *et seq.*

Count XLIV

Tennessee: Violation of HIPAA Safeguards

16
17
18 251. Plaintiff, Tennessee, incorporates the factual allegations in paragraphs 1 through
19 44 of this Complaint.

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

22
23 a. MIE failed to review and modify security measures needed to continue the
24 provision of reasonable and appropriate protection of ePHI in accordance with the
25 implementation specifications of the Security Rule, in violation of 45 C.F.R. §
26 164.306(e).

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

5
6 c. MIE failed to implement security measures sufficient to reduce risks and
7 vulnerabilities to a reasonable and appropriate level in accordance with the
8 implementation specifications of the Security Rule, in violation of 45 C.F.R. §
9 164.308(a)(1)(ii)(B).

10
11 d. MIE failed to implement procedures to regularly review records of
12 information system activity, such as audit logs, access reports, and Security Incident
13 tracking reports in accordance with the implementation specifications of the Security
14 Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D).

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

19
20 f. MIE failed to implement policies and procedures to address Security
21 Incidents, including suspected Security Incidents, to mitigate, to the extent practicable,
22 harmful effects of security incidents known to MIE, or to document such Incidents and
23 their outcomes in accordance with the implementation specifications of the Security Rule,
24 45 C.F.R. § 164.308(a)(6)(ii).

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

4 h. MIE failed to implement a mechanism to encrypt and decrypt ePHI, in
5 accordance with the implementation specifications of the Security Rule. 45 C.F.R. §
6 164.312(a)(2)(iv).

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

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

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

14 253. Plaintiff, Tennessee, is entitled to certain statutory damages pursuant to 42 U.S.C.
15 1320d-5(d)(2).

16
17
18
19 **Count XLV**

20 **Tennessee: Deceptive Acts in Violation of the Tennessee Consumer Protection Act, Tenn.
21 Code § 47-18-101 et seq.**

22 254. Plaintiff, Tennessee, incorporates the factual allegations in paragraphs 1 through
23 44 of this Complaint.

24 255. The Defendants' conduct constitutes a violation of Tenn. Code § 47-18-104.

25 256. The information security failings outlined in paragraphs 30 through 44 constitute
26 unfair or deceptive acts in violation of Tenn. Code § 47-18-104(a), (b)(5), (7), and (27).

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

Count XLVII
Tennessee: Failure to Make Reasonable Efforts to Protect Personal Information in Violation of Tenn. Code § 47-18-2110

264. Plaintiff, Tennessee, incorporates the factual allegations in paragraphs 1 through 44 of this Complaint.

265. Defendants failed to implement and maintain reasonable procedures to protect and safeguard the unlawful disclosure of personal information in violation of Tenn. Code § 47-18-2110(a) and (d).

266. The information security failings outlined in paragraphs 30 through 40 constitute unreasonable safeguard procedures in violation of Tenn. Code § 47-18-2110(a) and (d). Plaintiff, Tennessee, is entitled to civil penalties pursuant to Tenn. Code §§ 47-18-2110(d), 47-18-2106, and 47-18-108(b)(3), attorney fees and costs pursuant to Tenn. Code §§ 47-18-2110(d), 47-18-2105(f), 47-18-2106, and 47-18-108(b)(4), and injunctive relief pursuant to Tenn. Code §§ 47-18-2110(d), 47-18-2105(c), 47-18-2106, and 47-18-108(a)(1).

Count XLVIII
West Virginia: Violation of HIPAA Safeguards

267. Plaintiff, West Virginia, incorporates the factual allegations in paragraphs 1 through 44 of this Complaint.

268. 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

1 implementation specifications of the Security Rule, in violation of 45 C.F.R. §
2 164.306(e).

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

7
8 c. MIE failed to implement security measures sufficient to reduce risks and
9 vulnerabilities to a reasonable and appropriate level in accordance with the
10 implementation specifications of the Security Rule, in violation of 45 C.F.R. §
11 164.308(a)(1)(ii)(B).

12
13 d. MIE failed to implement procedures to regularly review records of
14 information system activity, such as audit logs, access reports, and Security Incident
15 tracking reports in accordance with the implementation specifications of the Security
16 Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D).

17
18 e. MIE failed to implement policies and procedures that, based upon its
19 access authorization policies, establish, document, review, and modify a user's right of
20 access to a workstation, transaction, program, or process that includes ePHI in
21 accordance with 45 C.F.R. § 164.308(a)(4)(ii)(C).

22
23 f. MIE failed to implement policies and procedures to address Security
24 Incidents, including suspected Security Incidents, to mitigate, to the extent practicable,
25 harmful effects of security incidents known to MIE, or to document such Incidents and
26 their outcomes in accordance with the implementation specifications of the Security Rule,
27 45 C.F.R. § 164.308(a)(6)(ii).

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

4 h. MIE failed to implement a mechanism to encrypt and decrypt ePHI, in
5 accordance with the implementation specifications of the Security Rule. 45 C.F.R. §
6 164.312(a)(2)(iv).

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

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

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

14
15
16
17
18 269. Plaintiff, West Virginia, is entitled to certain statutory damages pursuant to 42
19 U.S.C. 1320d-5(d)(2).

20 **Count XLIX**

21 **West Virginia: Deceptive Acts in Violation of W. Va. Code § 46A-6-104**

22 270. Plaintiff, West Virginia, incorporates the factual allegations in paragraphs 1
23 through 44 of this Complaint.

24 271. The Defendants' conduct constitutes a violation of W. Va. Code § 46A-6-104.

25 272. The information security failings outlined in paragraphs 23 through 44 constitute
26 unfair or deceptive acts in violation of W. Va. Code § 46A-6-104.

1 implementation specifications of the Security Rule, in violation of 45 C.F.R. §
2 164.308(a)(1)(ii)(B).

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

7
8 e. MIE failed to implement policies and procedures that, based upon its
9 access authorization policies, establish, document, review, and modify a user's right of
10 access to a workstation, transaction, program, or process that includes ePHI in
11 accordance with 45 C.F.R. § 164.308(a)(4)(ii)(C).

12
13 f. MIE failed to implement policies and procedures to address Security
14 Incidents, including suspected Security Incidents, to mitigate, to the extent practicable,
15 harmful effects of security incidents known to MIE, or to document such Incidents and
16 their outcomes in accordance with the implementation specifications of the Security Rule,
17 45 C.F.R. § 164.308(a)(6)(ii).

18
19 g. MIE failed to assign a unique name and/or number for identifying and
20 tracking user identity in accordance with the implementation specifications of the
21 Security Rule. 45 C.F.R. § 164.312(a)(2)(i).

22
23 h. MIE failed to implement a mechanism to encrypt and decrypt ePHI, in
24 accordance with the implementation specifications of the Security Rule. 45 C.F.R. §
25 164.312(a)(2)(iv).

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

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

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

8
9 277. Plaintiff, Wisconsin, is entitled to certain statutory damages pursuant to 42 U.S.C.
10 1320d-5(d)(2).

11
12 **Count LI**
13 **Wisconsin: Fraudulent Representations in Violation of Wis. Stat. § 100.20**

14 278. Plaintiff, Wisconsin, incorporates the factual allegations in paragraphs 1 through
15 44 of this Complaint.

16 279. The Defendants' conduct constitutes a violation of Wis. Stat. § 100.18.

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

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

22
23 **Count LII**
24 **Wisconsin: Negligent Disclosure of Patient Health Care Records in Violation of**
25 **Wis. Stat. § 146.84(2)(b)**

26 282. Plaintiff, Wisconsin, incorporates the factual allegations in paragraphs 1 through
27 44 of this Complaint.

1 283. The Defendants negligently disclosed confidential information in violation of
 2 Wis. Stat. § 146.82.

3 284. Plaintiff, Wisconsin, is entitled to civil penalties pursuant to Wis. Stat. §
 4 146.84(2)(b).
 5

6 **THIS COURT’S POWER TO GRANT RELIEF**

7
 8 285. Pursuant to 28 U.S.C. § 1367, this Court has supplemental jurisdiction to allow
 9 the Plaintiff States to enforce their state laws against Defendants in this Court and to grant such
 10 relief as provided under the following state laws including injunctive relief, civil penalties,
 11 attorneys’ fees, expenses, costs, and such other relief to which the Plaintiff States may be
 12 entitled:
 13

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 and 4-88-101 <i>et seq.</i>	Ark. Code Ann. §§ 4-110-108 and 4-88-101 <i>et seq.</i>
Connecticut:	Conn. Gen. Stat. § 42-110b, <i>et seq.</i>	Conn. Gen. Stat. § 36a-701b	Conn. Gen. Stat. § 42-471
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		

1	Louisiana:	La. Rev. Stat. § 51:1401 et seq.	La. Rev. Stat. 51:3071 et seq.	
2				
3	Michigan:	Mich. Comp. Laws § 445.905	Mich. Comp. Laws § 445.72(13)	
4				
5	Minnesota:	Minn. Stat. § 8.31	Minn. Stat. § 8.31	
6				
7	Nebraska:	Neb. Rev. Stat. §§ 59- 1602; 59-1608, and 59- 1614	Neb. Rev. Stat. § 87- 806	
8	North Carolina	N.C. Gen. Stat. § 75-1.1, <i>et seq.</i>	N.C. Gen. Stat. § 75-65	N.C. Gen. Stat. § 75-60, <i>et seq.</i>
9				
10				
11	Tennessee:	Tenn. Code § 47-18-108	Tenn. Cod Ann. §§ 47- 18-2105, 47-18-2016	Tenn. Code §§ 47- 18-2110, 47-18- 2105, and 47-18- 2016
12				
13	West Virginia:	W.Va. Code §§ 46A-1- 101 <i>et seq.</i> , 46A-7-108, and 46A-7-111		
14				
15	Wisconsin:	Wis. Stat. §§ 93.20, 100.18, and 100.26		Wis. Stat. § 146.84(2)(b)
16				
17				
18				

PRAYER FOR RELIEF

WHEREFORE, the Plaintiff States respectfully request that the Court:

- A. Award Plaintiffs such injunctive relief as permitted by statute;
- 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/ 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
Michael.Eades@atg.in.gov
Douglas.Swetnam@atg.in.gov

1 Attorney General Mark Brnovich

2 By: /s/ John C. Gray
3 John C. Gray (Pro Hac Vice)
4 Assistant Attorney General
5 Office of Attorney General Mark Brnovich
6 2005 N. Central Ave.
7 Phoenix, AZ 85004
8 Email: John.Gray@azag.gov
9 Telephone: (602) 542-7753
10 Attorney for Plaintiff State of Arizona

11 Attorney General Leslie Rutledge

12 By: /s/ Peggy Johnson
13 Peggy Johnson (Pro Hac Vice)
14 Assistant Attorney General
15 Office of Attorney General Leslie Rutledge
16 323 Center St., Suite 200
17 Little Rock, AR 72201
18 Email: peggy.johnson@arkansasag.gov
19 Telephone: (501) 682-8062
20 Attorney for Plaintiff State of Arkansas

21 Attorney General William Tong

22 By: /s/ Michele Lucan
23 Michele Lucan (Pro Hac Vice)
24 Assistant Attorney General
25 Office of Attorney General William Tong
26 110 Serman Street
27 Hartford, CT 06105
28 Email: michele.lucan@ct.gov
Telephone: (860) 808-5440
Attorney for Plaintiff State of Connecticut

1 Attorney General Ashley Moody

2 By: /s/ Diane Oates

3 Diane Oates (Pro Hac Vice)
4 Assistant Attorney General
5 Office of Attorney General Ashley Moody
6 110 Southeast 6th Street
7 Fort Lauderdale, FL 33301
8 Email: Diane.Oates@myfloridalegal.com
9 Telephone: (954) 712-4603
10 Attorney for Plaintiff State of Florida

11 By: /s/ Patrice Malloy

12 Patrice Malloy (Pro Hac Vice)
13 Bureau Chief, Multistate and Privacy Bureau
14 Florida Office of the Attorney General
15 110 SE 6th Street
16 Fort Lauderdale, FL 33301
17 (954) 712-4669
18 Patrice.Malloy@myfloridalegal.com

19 Attorney General Tom Miller

20 By: /s/ William Pearson

21 William Pearson (Pro Hac Vice)
22 Assistant Attorney General
23 Office of Attorney General Tom Miller
24 1305 E. Walnut, 2nd Floor
25 Des Moines, IA 50319
26 Email: William.Pearson@ag.iowa.gov
27 Telephone: (515) 281-3731
28 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

1 Attorney General Andy Beshear

2 By: /s/ Kevin R. Winstead
3 Kevin R. Winstead (Pro Hac Vice)
4 Assistant Attorney General
5 Office of Attorney General Andy Beshear
6 1024 Capital Center Drive
7 Frankfort, KY 40601
8 Email: Kevin.Winstead@ky.gov
9 Telephone: (502) 696-5389
10 Attorney for Plaintiff Commonwealth of Kentucky

11 Attorney General Jeff Landry

12 By: /s/ Alberto A. De Puy
13 Alberto A. De Puy (Pro Hac Vice)
14 Assistant Attorney General
15 Office of Attorney General Jeff Landry
16 1885 N. Third St.
17 Baton Rouge, LA 70802
18 Email: DePuyA@ag.louisiana.gov
19 Telephone: (225) 326-647

20 By: /s/ L. Christopher Styron
21 L. Christopher Styron (Pro Hac Vice)
22 Assistant Attorney General
23 Office of Attorney General Jeff Landry
24 1885 N. Third St.
25 Baton Rouge, LA 70802
26 Email: styronl@ag.louisiana.gov
27 Telephone: (225) 326-6400
28 Attorneys for Plaintiff State of Louisiana

Attorney General Dana Nessel

22 By: /s/ Kathy Fitzgerald
23 Kathy Fitzgerald (Pro Hac Vice)
24 Assistant Attorney General
25 Department of Attorney General Dana Nessel
26 Corporate Oversight Division
27 525 W. Ottawa St., 5th Floor
28 Lansing, MI 48933
Email: fitzgeraldk@michigan.gov
Telephone: (517) 335-7632
Attorney for Plaintiff State of Michigan

1 Attorney General Keith Ellison

2 By: /s/ Jason T. Pleggenkuhle
3 Jason T. Pleggenkuhle (Pro Hac Vice)
4 Assistant Attorney General
5 Office of Attorney General Keith Ellison
6 Bremer Tower, Suite 1200
7 445 Minnesota St.
8 St. Paul, MN 55101-2130
9 Email: jason.pleggenkuhle@ag.state.mn.us
10 Telephone: (651) 757-1147
11 Attorney for Plaintiff State of Minnesota

12 Attorney General Doug Peterson

13 By: /s/ Daniel J. Birdsall
14 Daniel J. Birdsall (Pro Hac Vice)
15 Assistant Attorneys General
16 Office of Attorney General Doug Peterson
17 2115 State Capitol
18 PO Box 98920
19 Lincoln, NE 68509
20 Email: dan.birdsall@nebraska.gov
21 Telephone: (402) 471-1279
22 Attorney for Plaintiff State of Nebraska

23 Attorney General Joshua H. Stein

24 By: /s/ Kimberley A. D'arruda
25 Kimberley A. D'Arruda (Pro Hac Vice)
26 Special Deputy Attorney General
27 North Carolina Department of Justice
28 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 Herbert Slattery III

29 By: /s/ Carolyn U. Smith
30 Carolyn U. Smith (Pro Hac Vice)
31 Senior Assistant Attorney General
32 Office of the Attorney General and Reporter Herbert H. Slattery III
33 P.O. Box 20207

1 Nashville, TN 37202-0207
2 Email: Carolyn.smith@ag.tn.gov
3 Telephone: (615) 532-2578
4 Attorney for Plaintiff State of Tennessee

5 Attorney General Patrick Morrisey

6 By: /s/ Tanya L. Godfrey
7 Tanya L. Godfrey (Pro Hac Vice)
8 Assistant Attorney General
9 Office of the West Virginia Attorney General Patrick Morrisey
10 269 Aikens Center
11 Martinsburg, WV 25404
12 Email: tanya.l.godfrey@wvago.gov
13 Telephone: (304) 267-0239
14 Attorney for Plaintiff State of West Virginia

15 Attorney General Josh Kaul

16 By: /s/ R. Duane Harlow
17 R. Duane Harlow (Pro Hac Vice)
18 Assistant Attorney General
19 Director, Consumer Protection and Antitrust Unit
20 Wisconsin Department of Justice
21 Office of Attorney General Josh Kaul
22 17 W. Main St., P.O. Box 7857
23 Madison, WI 53707-7857
24 Email: HarlowRD@doj.state.wi.us
25 Telephone: (608) 266-2950
26 Attorney for Plaintiff State of Wisconsin

27 **CERTIFICATE OF SERVICE**

28 I certify that on May 23, 2019 a copy of this document was served on all
counsel of record by operation of the Court's electronic filing system.

/s/ Michael A. Eades
Michael A. Eades, Deputy Attorney General
Data Privacy and Identity Theft Unit
Office of the Indiana Attorney General