

ANDREW J. BRUCK
ACTING ATTORNEY GENERAL OF NEW JERSEY
Division of Law
124 Halsey Street, 5th Floor
P.O. Box 45029
Newark, New Jersey 07101
Attorney for the New Jersey Division of Consumer Affairs

FILED

October 12 2021

Division of Consumer Affairs

By: Cody I. Valdez
Deputy Attorney General
(973) 648-4441

STATE OF NEW JERSEY
DEPARTMENT OF LAW AND PUBLIC
SAFETY DIVISION OF CONSUMER AFFAIRS

In the Matter of

DIAMOND INSTITUTE FOR
INFERTILITY AND MENOPAUSE,
LLC,

Respondent.

Administrative Action

CONSENT ORDER

WHEREAS this matter having been opened by the New Jersey Division of Consumer Affairs, Office of Consumer Protection (“Division”), as an investigation to ascertain whether violations of the New Jersey Consumer Fraud Act, N.J.S.A. 56:8-1 et seq. (“CFA”), the New Jersey Identity Theft Prevention Act, N.J.S.A. 56:8-161 et seq. (“ITPA”), and/or the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936, as amended by the Health Information Technology for Economic and Clinical Health Act, Pub. L. No. 111-5, 123 Stat. 226, and the Department of Health and Human Services Regulations, 45 C.F.R. § 160 to 180 (collectively, “HIPAA”) have been or are being committed (the “Investigation”) by Diamond Institute for Infertility and Menopause L.L.C. (“Diamond”).

WHEREAS the Attorney General is charged with the responsibility of enforcing the CFA and the ITPA, and the Director of the Division is charged with administering the CFA on behalf of the Attorney General;

WHEREAS the Attorney General, as *parens patriae* for the State of New Jersey and in its sovereign capacity, may, pursuant to 42 U.S.C. § 1320d-5(d), enforce the provisions of HIPAA;

WHEREAS Diamond is a Millburn, New Jersey-based company that focuses on the diagnosis and treatment of infertility;

WHEREAS the Division alleges that Diamond engaged in conduct in violation of the CFA and HIPAA in connection with the improper handling of, and unreasonable security measures implemented to secure Personal Information, Protected Healthcare Information, and/or Electronic Protected Healthcare Information stored on its workstations and third-party servers from August 28, 2016 through January 14, 2017, affecting approximately 11,071 New Jersey residents;

WHEREAS the Division alleges that Diamond failed to execute Business Associate Agreements with multiple Business Associates handling Protected Healthcare Information; and

WHEREAS the Division and Diamond (collectively, the “Parties”) have reached an amicable agreement resolving the issues in controversy and concluding the Investigation without the need for further action, and Diamond having cooperated with the Investigation and consented to the entry of the within order (“Consent Order”) without admitting any violation of law, and for good cause shown;

IT IS ORDERED AND AGREED as follows:

1. EFFECTIVE DATE

1.1 This Consent Order is effective on the date that it is filed with the Division, which filing date the Division Clerk stamps on the executed Consent Order (“Effective Date”).

2. DEFINITIONS

As used in this Consent Order, the following words or terms shall have the following meanings, which shall apply wherever the words or terms appear in this Consent Order:

2.1 “Attorney General” shall refer to the Attorney General of the State of New Jersey and the Office of the Attorney General of the State of New Jersey.

2.2 “Breach” shall refer to the Security Incident, and all events related thereto, discovered by Diamond on or about January 14, 2017, and publicly announced on April 28, 2017, in which an individual(s) gained unauthorized access to portions of the Diamond Network that stored PI, PHI and/or ePHI, and which impacted approximately 14,633 individuals nationwide.

2.3 “Breach Notification Rule” shall refer to 45 C.F.R. Part 160 and 45 C.F.R. Part 164, Subparts A and D.

2.4 “Business Associate” shall be defined in accordance with 45 C.F.R. § 160.103.

2.5 “Business Associate Agreement” or “BAA” shall mean the contract or other written arrangement required by 45 C.F.R. § 164.502(e)(2) and meets the requirements of 45 C.F.R. §164.504(e).

2.6 “Covered Entity” shall be defined in accordance with 45 C.F.R. § 160.103.

2.7 “Covered Systems” shall mean components, such as servers, workstations, and devices, within the Diamond Network that are routinely used to collect, process, communicate, and/or store PI and/or ePHI.

2.8 “Cyber Security Operations Center” or “C-SOC” shall mean the employment of person(s), processes, and technology to continuously monitor and update Diamond’s security posture while preventing, detecting, analyzing, and responding to security incidents.

2.9 “Division” or “Division of Consumer Affairs” shall refer to the New Jersey Division of Consumer Affairs.

2.10 “Diamond” shall mean Diamond Institute for Infertility and Menopause L.L.C. its wholly owned, integrated, and operated affiliates, subsidiaries, and divisions, successors, and assigns, directors and officers, and employees doing business in the United States.

2.11 “Diamond Network” shall mean the networking equipment, databases or data stores, applications, servers, workstations, and endpoints that are capable of using and sharing software, data, and hardware resources and that are owned and/or operated by Diamond.

2.12 “Diamond Privacy Policy” refers to the HIPAA Privacy Policy & Procedure Manual for Diamond that became effective on July 1, 2020 and is to be reviewed yearly.

2.13 “Diamond Security Policy” refers to the HIPAA Security Policy & Procedure Manual for Diamond that became effective on July 1, 2020 and is to be reviewed yearly.

2.14 “Electronic Protected Health Information” or “ePHI” shall be defined in accordance with 45 C.F.R. § 160.103.

2.15 “Encrypt,” “Encrypted,” or “Encryption” shall refer to the transformation of data at rest or in transit into a form in which meaning cannot be assigned without the use of a confidential process or key. The manner of Encryption shall conform to the existing industry standard.¹

2.16 “Minimum Necessary Standard” shall refer to the requirements of the Privacy Rule that, when using or disclosing PHI or when requesting PHI from another Covered Entity or Business Associate, a Covered Entity or Business Associate must make reasonable efforts to limit

¹ For the purposes of this Consent Order, the term “existing industry standard” applies to what the standard may become as the industry changes over time. As of the Effective Date, the existing industry standard shall be defined pursuant to Federal Information Processing Standards Publication 140-2.

PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request as defined in 45 C.F.R. § 164.502(b) and § 164.514(d)(1)-(5).

2.17 “Multi-factor Authentication” means authentication through verification of at least two of the following authentication factors: (i) knowledge factors such as a password; or (ii) possession factors, such as a token, connection through a known authenticated source, or a text message on a mobile phone; or (iii) inherent factors, such as biometric characteristics.

2.18 “New Jersey” or “State” shall refer to the State of New Jersey.

2.19 “Panurgy” shall refer to Panurgy, an IT service provider, with whom Diamond entered into the Panurgy Total Support/PTDP Service contract on November 10, 2017, which provides an integrated and proactive approach for managing and monitoring the Diamond Network, and includes services to protect the Diamond Network from interruptions, ensuring business continuity, confirming backups, and reducing security risks.

2.20 “Personal Information” or “PI” shall mean the data elements in the definition of personal information set forth in the Identity Theft Protection Act, N.J.S.A. 56:8-161 to -166.3.

2.21 “Privacy Rule” shall refer to 45 C.F.R. Part 160 and 45 C.F.R. Part 164, Subparts A and E.

2.22 “Privileged User Queries” shall mean any search within the Diamond Network that allows the user to have access to documents or files containing PHI or ePHI.

2.23 “Protected Health Information” or “PHI” shall be defined in accordance with 45 C.F.R. § 106.103.

2.24 “Security Incident” shall be defined in accordance with 45 C.F.R. § 106.103.

2.25 “Security Information and Event Management” and “SIEM” shall mean software and/or services that carry out analysis of event and log data in real-time to provide event

correlation, threat monitoring, and incident response, as well as retrieve and analyze log data and generate a report, such as the analytical software tools and services described in Diamond's November 10, 2017 contract with Panurgy.

2.26 "Security Rule" shall refer to 45 C.F.R. Part 160 and 45 C.F.R. Part 164, Subparts A and C.

3. STIPULATED FACTS

3.1 Diamond is an independent, privately owned corporation devoted to the diagnosis and treatment of infertility that owns and operates two healthcare practices located in New Jersey, one healthcare practice in New York, and offers consultation services at a healthcare practice in Bermuda.

3.2 Diamond was organized as a New Jersey professional association in 1972 and as a limited liability company in 1997, and maintains a principal business address at 89 Millburn Avenue, Millburn, New Jersey 07041.

3.3 At all relevant times, Diamond is and has been a Covered Entity within the meaning of HIPAA.

3.4 As a Covered Entity, Diamond is required to comply with the HIPAA federal standards that govern the privacy of PHI, including the Privacy Rule and the Security Rule.

3.5 On January 31, 2007, Diamond entered into an "On-site 'Gold' Support" managed services agreement with Infoaxis Technologies Inc. ("Infoaxis") to provide security and information technology services for Diamond, including, but not limited to, maintaining its third-party server and workstations. This managed services agreement included third-party software for the management and reporting of audit logs intended to interpret triggers for event alerts.

3.6 In or around March 2014, Diamond changed the managed services agreement with Infoaxis from the “On-site ‘Gold’ Support” agreement to the “Essentials+” agreement. The “Essentials+” agreement did not include all the same services as the “On-site ‘Gold’ Support” agreement.

3.7 Diamond alleges that there was no reduction in services from the “On-site ‘Gold’ Support” agreement to the “Essentials+” agreement other than the amount of time included in the plan for on-site support services.

3.8 Prior to the Breach, Diamond’s HIPPA Privacy and Security Officer (“HPSO”) utilized a Remote Desktop Protocol (“RDP”) service with a virtual private network (“VPN”) to access the Diamond Network. However, because Diamond’s VPN was blocked from its Bermuda office, Infoaxis provided Diamond with an alternative method of remote access, which resulted in Infoaxis opening a port in Diamond’s firewall for RDP access, rather than using the VPN for authentication.

3.9 Over the course of five and a half months, from August 28, 2016 through January 14, 2017, the Millburn office workstation of Diamond’s HPSO was remotely accessed by undetected intruder(s) a significant number of times from foreign IP addresses. Unauthorized access was first discovered on January 14, 2017, when Infoaxis confirmed that an unauthorized user remotely accessed Diamond’s HPSO’s Millburn Office workstation.

3.10 During the period of unauthorized access, the data on the compromised workstation was not Encrypted. As a result, the intruder(s) had the ability to access ePHI stored on the workstation, including patients’ first and last names, dates of birth, Social Security Numbers, and medical record numbers.

3.11 Diamond’s review of the Breach determined that at least one intruder also accessed Diamond’s third-party server, which housed Diamond’s electronic medical records (“EMR”) data within a password protected Microsoft SQL database. Diamond’s investigation determined that the unauthorized access occurred through two compromised Diamond user accounts, which at the time of the Breach had weak passwords. Diamond also had weak security settings for failed login attempts, and password expiration.

3.12 Diamond did not Encrypt any of the ePHI stored on the third-party server. While the EMR data stored within the password protected Microsoft SQL database was not affected, the intruder was capable of accessing unprotected patient documents, which included patient lab results, ultrasound images and reports, clinical notes, and post-operative notes.

3.13 Diamond’s investigation of the Breach revealed that 14,663 Diamond Institute patients, including 11,071 New Jersey residents, had PI and ePHI that was potentially accessed by the intruder(s).

3.14 Diamond’s investigation was unable to determine how the intruder(s) gained access to the Diamond network.

3.15 Diamond notified the New Jersey Division of State Police and the affected population of the Breach on April 28, 2017.

3.16 During the relevant time period, Diamond either did not have Business Associate Agreements in place or does not have documentation of Business Associate Agreements being in place, prior to it sharing ePHI with its Business Associates, Berkshire Medical Technologies (“BMedTech”), Infoaxis, and Igenomix.

3.17 Diamond stipulates to the enumerated facts stated in Section 3 for purposes of this Consent Order only.

4. ALLEGED VIOLATIONS OF LAW

4.1 The Division has alleged the following:

- a. At all relevant times set forth in Section 3 above (the “Relevant Time Period”), incorporated herein by reference, Diamond was and continues to be a Covered Entity.
- b. During the Relevant Time Period, Infoaxis, BMedTech, and Igenomix were Business Associates of Diamond.
- c. As a Covered Entity, Diamond was, and continues to be, required to comply with HIPAA standards governing the privacy and security of PHI and/or ePHI, including, but not limited to the Security Rule and the Privacy Rule.
- d. Diamond violated the CFA, HIPAA’s Security Rule, and HIPAA’s Privacy Rule when it removed administrative and technological safeguards protecting PHI and ePHI resulting in the unauthorized access to the Diamond Network left undetected for approximately five and a half months.
- e. Specifically, Diamond failed to comply with the Security Rule and Privacy Rule by:
 - failing to ensure the confidentiality, integrity, and availability of ePHI, in violation of 45 C.F.R. § 164.306(a)(1);
 - failing to protect against reasonably anticipated threats or hazards to security or integrity of ePHI, in violation of 45 C.F.R. § 164.306(a)(2);
 - failing to review and modify security measures as needed to continue reasonable and appropriate protection of ePHI, in violation of 45 C.F.R. § 164.306(e);
 - failing to conduct an accurate and thorough risk assessment of potential risk and vulnerabilities to the

confidentiality, integrity, and availability of ePHI, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(A);

- failing to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a), in violation of 45 C.F.R. § 164.308(a)(1)(ii)(B);
- failing to implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);
- failing to implement procedures to determine that the access of a workforce member to ePHI was appropriate, or document why the implementation of such procedures were not reasonable or appropriate, and implement an equivalent alternative measure, in violation of 45 C.F.R. § 164.308(a)(3)(ii)(B);
- failing to make reasonable efforts to implement proper specifications of the “minimum necessary requirements,” in violation of 45 C.F.R. § 164.502(b) and 45 C.F.R. § 164.514(d)(2)(i)(A)-(B);
- failing to implement proper procedures for creating, changing, and safeguarding passwords, or document why the implementation of such procedures were not reasonable or appropriate, and implement an equivalent alternative measure, in violation of 45 C.F.R. § 164.308(a)(5)(ii)(D);
- failing to implement proper procedures for creating and maintaining retrievable exact copies of ePHI, in violation of 45 C.F.R. § 164.308(a)(7)(ii)(A);
- failing to implement procedures for periodic testing and revision of contingency plans, or document why the implementation of such procedures were not reasonable or appropriate, and implement an equivalent alternative, in violation of 45 C.F.R. § 164.308(a)(7)(ii)(D);
- failing to assess the relative criticality of specific application and data in support of other contingency plan components, or document why implementation of such procedures were not reasonable or appropriate, and

implement an equivalent alternative, in violation of 45 C.F.R. § 164.308(a)(7)(ii)(E);

- failing to assign a unique name and/or number for identifying and tracking user identity, in violation of 45 C.F.R. § 164.312(a)(2)(i);
- failing to implement a mechanism to Encrypt ePHI, or document why implementation of such a mechanism was not reasonable or appropriate, and implement an equivalent alternative measure, in violation of 45 C.F.R. § 164.312(a)(2)(iv);
- failing to implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI, in violation of 45 C.F.R. § 164.312(b);
- failing to implement electronic mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner, or document why implementation of such a mechanism was not reasonable or appropriate, and implement an equivalent alternative measure, in violation of 45 C.F.R. § 164.312(c)(2);
- failing to implement procedures to verify that the person seeking access to ePHI is who they claim, in violation of 45 C.F.R. § 164.312(d);
- failing to review and update its policies and procedures in response to environmental or operational changes affecting the security of ePHI, in violation of 45 C.F.R. § 164.316(b)(2)(iii);
- failing to implement a written contract or other arrangement with three (3) Business Associates to document that it has obtained satisfactory assurances that the Business Associates will appropriately safeguard the ePHI, and shared ePHI with entities despite this failure, resulting in violations of 45 C.F.R. § 164.308(b)(1); 45 C.F.R. § 164.308(b)(3); 45 C.F.R. § 164.314(a)(2)(i)(A)-(C); 45 C.F.R. § 164.502(a)(1)(iii); 45 C.F.R. § 164.502(e)(1); 45 C.F.R. § 164.502(e)(2); 45 C.F.R. § 164.504(e); and 45 C.F.R. § 164.530(c)(2)(i); and

- failing to appropriately sanction its Security Officer for not complying with its privacy and security policies, in violation of 45 C.F.R. § 164.530(e) and 45 C.F.R. § 164.308(a)(1)(ii)(C).
- f. At all relevant times, Diamond has offered for Sale and Sold services that are Merchandise within the meaning of the CFA.
- g. Diamond engaged in violations of the CFA by misrepresenting its HIPAA practices in its security policy and privacy policy.
- h. Diamonds' failure to ensure the proper security of the Diamond Network, which led to the Breach exposing approximately 11,071 New Jersey customers' ePHI, constitutes separate and additional unconscionable commercial practices, in violation of CFA, N.J.S.A. 56:8-2.

4.2 The Division has alleged that Diamond's conduct described in Section 4.1 constitute separate and additional unconscionable commercial practices in violation of the CFA, N.J.S.A. 56:8-2.

4.3 Diamond disputes the allegations set forth in Section 4.1 and Section 4.2.

5. AGREED-UPON BUSINESS PRACTICES

A. Compliance with State and Federal Law

5.1 Diamond shall not engage in conduct in violation of the CFA, ITPA, and HIPAA, including the Privacy Rule, Breach Notification Rule and/or Security Rule, in connection with the security, collection, use, disclosure, storage, or disposal of PI, PHI, or ePHI.

5.2 Diamond shall not misrepresent the extent to which Diamond maintains and protects the privacy, security, or confidentiality of PI, PHI, or ePHI collected from or about consumers.

5.3 If a Security Incident does not trigger the Breach Notification Rule, Diamond shall create a report that includes a description of the Security Incident and Diamond's response to that Security Incident ("Security Incident Report"), in accordance with the Diamond Privacy Policy, and the Diamond Security Policy. The Security Incident Report shall be made available for inspection by the Third-Party Security Assessor as described in Paragraph 5.21.

5.4 Diamond shall execute Business Associate Agreements with each current Business Associate within thirty (30) days of the Effective Date, if not already executed as of the Effective Date.

B. Information Security Program

5.5 Diamond shall develop, implement, and maintain a written information security program ("Information Security Program") that is reasonably designed to protect the security, integrity, and confidentiality of PI and PHI that Diamond collects, stores, transmits, maintains, and/or destroys. The Information Security Program shall, at minimum, include the specific information requirements set forth in Paragraphs 5.6 through 5.20 of this Consent Order.

a. As discussed here, the Information Security Program shall comply with any applicable requirements under State or federal law, and shall contain administrative, technical, and physical safeguards appropriate to: (i) the size and complexity of Diamond's operations; (ii) the nature and scope of Diamond's activities; and (iii) the sensitivity of the PI, PHI, and ePHI that Diamond collects, stores, transmits and/or maintains.

b. The Information Security Program shall be written and modified to allow access to PHI and ePHI consistent with the Minimum Necessary Standard, and in accordance with the Diamond Privacy Policy, and the Diamond Security Policy. In accordance with the Diamond Security Policy, Diamond shall:

i. Regularly monitor, log, and inspect network traffic, including log-in attempts, through the implementation of hardware, software, or procedural mechanisms that record and evaluate such activity;

ii. Authorize and authenticate relevant device, user, and network activity within the Diamond Network; and

iii. Require appropriate authorization and authentication prior to any user's access to the Diamond Network.

c. Diamond may satisfy the requirements of this Consent Order, including the implementation of the Information Security Program through the review, maintenance, and if necessary, updating of its existing information security program and existing safeguards, provided that such existing program and safeguards meet the requirements set forth in this Consent Order.

d. Diamond shall review not less than annually the Information Security Program.

e. Diamond shall appoint and maintain an employee, other than Diamond's HPSO at the time of the Breach, who shall serve as its HPSO and be responsible for implementing, maintaining, and monitoring the Information Security Program within sixty (60) days from the Effective Date, if not already appointed as of the Effective Date. The HPSO shall have the background and expertise, with documentation of her or his background and expertise, in information security appropriate to the level, size, and complexity of her or his role in implementing, maintaining, and monitoring the Information Security Program.

f. Within thirty (30) days of the employment of the HPSO, Diamond shall provide a statement, in writing to the Division that it has designated an HPSO. This writing shall

also include the name of the HPSO for Diamond and documentation of her or his background and expertise.

g. The role of the HPSO will include regular and direct reporting to Diamond's Executive Staff and Directors concerning Diamond's security posture, the security risks faced by Diamond, and the security implications of Diamond's business decisions. The HPSO shall meet and provide a report to Diamond's Executive Staff and Directors on at least a quarterly basis. The HPSO shall report to Diamond's Directors within twenty-four (24) hours of a confirmed Security Incident impacting 500 or more consumers residing in the United States.

h. Diamond shall provide notice of the requirements of this Consent Order to its employee(s) and shall implement training on the requirements of this Consent Order. Diamond shall provide the training required under this paragraph to its employees within ninety (90) days of the Effective Date of this Consent Order or prior to their handling of any PHI or ePHI.

i. As part of its Information Security Program, Diamond shall develop, implement, and maintain a written incident response plan to prepare for and respond to Security Incidents. Diamond shall revise and update this response plan, as necessary, to adapt to any material changes that affect the security of PI, PHI, and ePHI. Such a plan shall, at a minimum, identify and describe the following phases: (i) Preparation; (ii) Detection and Analysis; (iii) Containment; (iv) Notification and Coordination with Law Enforcement; (v) Eradication; (vi) Recovery; (vii) Consumer and Regulator Notification and Remediation; and (viii) Post-Incident Analysis.

j. Diamond shall ensure that its Information Security Program receives the resources and support reasonably necessary to function as intended.

C. Specific Information Security Requirements

5.6 **Data Collection & Retention:** Diamond shall develop, implement, and maintain reasonable policies and procedures governing its collection, use, and retention of PI, PHI, and ePHI. Diamond shall limit its use, disclosure of, and requests for PHI and ePHI in accordance with the Minimum Necessary Standard, to fulfill all applicable State and federal regulatory, legal, and contractual obligations.

5.7 **Cyber Security Operations Center:** Diamond shall maintain the existence and operation of a C-SOC, or third-party IT vendor that performs services reasonably equivalent to a C-SOC. The C-SOC or reasonably equivalent third-party IT vendor shall provide comprehensive monitoring of servers and other technologies to identify improper use of data, including PI, PHI, and/or ePHI. The C-SOC's or reasonably equivalent third-party IT vendor's analytic capabilities shall be deployed to detect, analyze, and respond to potential and confirmed Security Incidents.

5.8 **Logging & Monitoring:** Diamond shall develop, implement, and maintain reasonable policies and procedures designed to properly log and monitor the Diamond Network. At a minimum:

a. Diamond shall employ tools, either through the C-SOC or third-party IT vendor that performs services reasonably equivalent to a C-SOC, such as a Security Information and Event Monitoring solution ("SIEM") (or a reasonably equivalent technology), among others, to log and monitor network traffic to detect and respond to Security Incidents.

b. Diamond shall take reasonable steps to ensure the SIEM (or reasonably equivalent technology) used pursuant to subsection (a) is properly configured, and regularly updated or maintained, and shall take reasonable steps to adequately log system activity and identify potential Security Incidents for review. Using the SIEM (or a reasonably equivalent

technology), Diamond shall actively review and analyze in real-time the logs of system activity and take appropriate follow-up actions with respect to Security Incidents.

c. Diamond shall maintain logs of system activity in conformance with industry standards and all applicable State and federal laws.

d. In addition to the requirements set forth in subparagraphs (a) through (c) of this paragraph, Diamond shall implement, and maintain defined and specific policies and procedures with respect to logging and monitoring of any database (or set of databases) that collects, processes, transmits, and/or stores PI, PHI, and/or ePHI, in accordance with the Diamond Privacy Policy and Diamond Security Policy. At a minimum:

i. Diamond shall either through the C-SOC or third-party IT vendor that performs services reasonably equivalent to a C-SOC, deploy an appropriate database activity monitoring tool or a reasonably equivalent technology in any database (or set of databases) that Diamond uses to collect, process, transmit, and/or store PI and/or PHI, to the extent it is commercially feasible.

ii. The monitoring of such database(s) shall include commercially reasonable query categories available in a database activity monitoring tool or reasonable equivalent issued to the relevant database(s).

iii. The monitoring of such database(s) shall be performed by appropriately trained and experienced personnel.

e. Diamond shall create a formalized procedure to track Security Incidents and alerts on Privileged User Queries on a regular basis and document identified issues as necessary action items.

5.9 **Antivirus Maintenance:** Diamond shall implement and maintain current, up-to-date antivirus protection programs or a reasonably equivalent technology on the Diamond Network components.

5.10. **Access Controls:** Diamond shall implement and maintain appropriate controls to manage access to and use of all accounts with access to PI, PHI, or ePHI, including individual accounts, administrator accounts, service accounts, and vendor accounts. Such controls shall include a means to regularly review access and access levels of users and remove network and remote access at the time of notification of termination for any employee whose employment has ended or any non-associate whose term has ended, in accordance with the Diamond Security Policy.

5.11 **Authentication:** Diamond shall implement and maintain reasonable policies and procedures requiring the use of authentication in accordance with industry standards, including as appropriate under industry standards, strong passwords, password rotation, and ensuring that stored passwords are protected from unauthorized access.

5.12 **Remote Access/Multi-factor Authentication:** Diamond shall require the use of Multi-factor Authentication or reasonably equivalent technology for end-user remote access to the Diamond Network.

5.13 **Encryption:** Diamond shall develop, implement, maintain, regularly review, and revise its policies and procedures to Encrypt PI and ePHI at rest and in transit as reasonable and appropriate, and in accordance with applicable law.

a. Diamond shall secure all of its EMR data, including lab results, ultrasound images and reports, clinical notes, and post-operative notes, with Encryption (or a reasonably equivalent technology) based upon industry standards.

5.14 **Asset Inventory:** Diamond shall develop, maintain, and regularly update a reasonable inventory of the assets that primarily comprise the Diamond Network and appropriately identify and secure assets containing PHI and ePHI.

5.15 **Risk Assessments:** Diamond shall develop, implement, and maintain a risk assessment program to identify, address, and as appropriate, remediate risks affecting its Covered Systems. At a minimum, Diamond shall have an annual risk assessment performed by an independent third party. The assessment shall include assessment of all reasonably anticipated, internal and external risks to the security, confidentiality, or availability of PI, PHI, and ePHI collected, processed, transmitted, stored, or disposed of by Diamond. Such reports shall be maintained by the HPSO, made available for inspection by the Third-Party Assessor described in paragraph 5.21 of this Consent Order, and a copy of the report shall be produced to the Division within ten (10) days of completion for a total period of seven (7) years.

5.16 **Email Filtering and Phishing Solutions:** Diamond shall maintain email protection and filtering solutions for all of Diamond's email accounts, including the filtering of SPAM, phishing attacks, and other email malware attacks.

5.17 **Employee Training:** In addition to the requirements set forth in Paragraph 5.5(h) above, Diamond shall conduct an initial training for all new employees no later than thirty (30) days after their employment and, on at least an annual basis, train existing employees concerning its information privacy and security policies, the proper handling and protection of PI, PHI, and ePHI, and disciplinary measures for violation, up to and including termination, in accordance with the Diamond Security Policy.

5.18 **Intrusion Detection and Prevention Solution(s):** Diamond shall develop, implement, and maintain an intrusion detection and prevention solution to assist in detecting and

preventing unauthorized access to the Diamond Network.

5.19 **Data Loss/Exfiltration Prevention:** Diamond shall develop, implement, and maintain a data loss prevention technology or a reasonably equivalent technology to detect and prevent unauthorized data exfiltration from the Diamond Network.

5.20 **Business Associate Agreements:** Prior to any disclosure of PHI and/or ePHI to a Business Associate, Diamond shall obtain satisfactory assurances that the Business Associate will appropriately safeguard the PHI and/or ePHI and shall document such assurances in a BAA, as required by 45 C.F.R. § 164.502(e)(1), 45 C.F.R. § 164.502(e)(2), and 45 C.F.R. § 164.504(e).

D. Information Security Program Assessment

5.21 Diamond shall obtain an information security assessment of its policies and practices pertaining to the collection, storage, maintenance, transmission, and disposal of PI and PHI, from an independent third-party professional (“Third-Party Assessor”) within ninety (90) days of the Effective Date of this Assurance and then once a year thereafter for a total period of seven (7) years.

5.22 The Third-Party Assessor must be an organization that employs at least one individual to perform the assessment that is: (a) qualified as a Certified Information System Security Professional (“CISSP”) or as a Certified Information Systems Auditor (“CISA”), or a similar qualification; and (b) has at least five (5) years of experience evaluating the effectiveness of computer systems of information system security.

5.23 The Third-Party Assessor shall review this Consent Order and the Security Incident Report and risk assessments provided by Diamond as set forth in Paragraphs 5.3 and 5.15 respectively. The Third-Party Assessor shall prepare a formal (“Security Report”) that shall confirm Diamond’s development, implementation, and maintenance of a written Information

Security Program with security controls and processes that meet the requirements of this Consent Order related to: antivirus maintenance and access controls including multi-factor authentication, logging and monitoring, Encryption, and information system activity review and detection. The Security Report shall also confirm that Diamond has complied with the provisions of this Consent Order related to the employment of an HPSO, maintenance of a C-SOC or third-party IT vendor that performs services reasonably equivalent to a C-SOC, and performance of information security training.

5.24 The initial Security Report shall be provided to the Division no later than one hundred eighty (180) days after the Effective Date, and each subsequent Security Report shall be submitted to the New Jersey Attorney General no later than ten (10) days after its completion. Diamond will also provide the Risk Assessment, as set forth in Paragraph 5.15, to the New Jersey Attorney General on an annual basis during the seven-year term.

a. Confidentiality: The Division, shall, to the extent permitted by State law, treat each Security Report as exempt from disclosure as applicable under the New Jersey Open Public Records Act, N.J.S.A. 47:1A-1 to -13.

5.25 Upon receipt of each Security Report, Diamond will review and evaluate whether to revise its current policies and procedures based on the findings of the Security Report. Within sixty (60) days of Diamond's receipt of each Security Report, Diamond shall forward to the Division a description of any action it plans to take, or if no action is taken, a detailed description why no action is necessary, in response to each Security Report.

6. SETTLEMENT PAYMENT

6.1 The Parties have agreed to a settlement of the Investigation in the amount of \$495,000.00 ("Settlement Payment"), to be paid to the Division within sixty (60) days upon the

effective date of the Settlement Agreement. This Settlement Payment consists of \$412,300.00 allocated to the Division's civil penalty claims, and \$82,700.00 allocated to the Division's claims for reimbursement of attorneys' fees and investigative costs. The allocation of the Settlement Payment is not a finding or admission by Diamond of liability for civil penalties or attorneys' fees and investigative costs.

6.2 Diamond shall make the Settlement Payment by wire transfer, credit card, or by certified check, cashier's check or money order made payable to the "New Jersey Division of Consumer Affairs" and forwarded to:

Case Initiation and Tracking Unit
New Jersey Department of Law and Public Safety
Division of Consumer Affairs
124 Halsey Street – 7th Floor
P.O. Box 45025
Newark, New Jersey 07101
Attention: Van Mallett, Lead Investigator

6.3 Upon making the Settlement Payment, Diamond shall immediately be fully divested of any interest in, or ownership of, the money paid. All interest in the Settlement Payment, and any subsequent interest or income derived therefrom, shall inure entirely to the benefit of the Division pursuant to the terms herein.

7. GENERAL PROVISIONS

7.1 This Consent Order is entered into by the Parties as their own free and voluntary act and with full knowledge and understanding of the obligations and duties imposed by this Consent Order.

7.2 This Consent Order shall be governed by, and construed and enforced in accordance with, the laws of the State of New Jersey.

7.3 The Parties have negotiated, jointly drafted, and fully reviewed the terms of this Consent Order and the rule that uncertainty or ambiguity is to be construed against the drafter shall not apply to the construction or interpretation of this Consent Order.

7.4 This Consent Order contains the entire agreement among the Parties. Except as otherwise provided herein, this Consent Order shall be modified only by a written instrument signed by or on behalf of the Parties.

7.5 Except as otherwise explicitly provided in this Consent Order, nothing herein shall be construed to limit the authority of the Attorney General to protect the interests of the State or the people of the State.

7.6 If any portion of this Consent Order is held invalid or unenforceable by operation of law, the remaining terms of this Consent Order shall not be affected.

7.7 This Consent Order shall be binding upon the Parties and their successors in interest. In no event shall assignment of any right, power, or authority under this Consent Order avoid compliance with this Consent Order.

7.8 This Consent Order is entered into by the Parties for settlement purposes only. Neither the fact of nor any provision contained in this Consent Order shall constitute or be construed as: (a) an approval, sanction, or authorization by the Attorney General, the Division, or any other governmental unit of the State of any act or practice of Diamond; or (b) an admission by Diamond that it violated the CFA, ITPA, or HIPAA, including the Privacy Rule, Breach Notification Rule, and/or the Security Rule, or any other federal or State law, administrative rule or regulation, or an express or implied admission of any other matter of fact or law, or of any liability or wrongdoing.

7.9 This Consent Order is not intended, and shall not be deemed, to constitute evidence or precedent of any kind in any action or proceeding except in: (a) an action or proceeding by one of the Parties to enforce, rescind, or otherwise implement any or all of the terms herein; or (b) an action or proceeding involving a Released Claim (as defined in Section 8) to support a defense of res judicata, collateral estoppel, release, or other theory of claim preclusion, issue preclusion, or similar defense.

7.10 The Parties represent and warrant that their signatories to this Consent Order have authority to act for and bind the respective Party.

7.11 Unless otherwise prohibited by law, any signatures by the Parties required for filing of this Consent Order may be executed in counterparts, each of which shall be deemed an original, but all of which shall constitute one and the same Consent Order. Electronic signatures shall constitute acceptable, binding signatures for purposes of this Consent Order.

8. RELEASE

8.1 In consideration of the undertakings, mutual promises, and obligations provided for in this Consent Order and conditioned on Diamond making the Settlement Payment as described in Section 6, the Division hereby agrees to release Diamond from any and all civil claims or causes of action, or consumer-related administrative claims or actions, to the extent permitted by law, which the Division could have brought prior to the Effective Date against Diamond for violations of any consumer protection law administered or enforced by the Division, CFA, ITPA, or HIPAA, including the Privacy Rule, Breach Notification Rule, and/or Security Rule, arising out of the Investigation, as well as the matters specifically addressed in this Consent Order (“Released Claims”).

8.2 Notwithstanding any term of this Consent Order, the following do not comprise

Released Claims: (a) private rights of action; (b) actions to enforce this Consent Order; and (c) any claims against Diamond by any other agency or subdivision of the State except any civil claims or causes of action, or consumer-related administrative claims or actions, arising out of the Investigation as well as the matters specifically addressed in this Consent Order that the Division could have brought but has released in Section 8.1 above.

9. PENALTIES FOR FAILURE TO COMPLY

9.1 The Attorney General (or designated representative) shall have the authority to enforce the provisions of this Consent Order or to seek sanctions for violations hereof or both.

9.2 Prior to filing any action to enforce the provisions of this Consent Order, the Attorney General (or designated representative) shall meet and confer with Diamond in an attempt to resolve any dispute with respect to compliance with this Consent Order. The Attorney General (or designated representative) shall notify Diamond in writing of the alleged violation of this Consent Order, and Diamond shall have fifteen (15) days to respond to the notification. The Attorney General (or designated representative) shall not file any action until the fifteen (15) days expires.

10. COMPLIANCE WITH ALL LAWS

10.1 Except as provided in this Consent Order, no provision herein shall be construed as:

- a. Relieving Diamond of its obligations to comply with all State and federal laws, regulations, or rules, as now constituted or as may hereafter be amended; granting permission to engage in any acts or practices prohibited by any such laws, regulations, or rules; or requiring Diamond s to take an action that is prohibited by such laws, regulations, or rules; or

- b. Limiting or expanding any right the Division may otherwise have to obtain information, documents, or testimony from Diamond pursuant to any State or federal law, regulation, or rule, as now constituted or as may hereafter be amended, or limiting or expanding any right Diamond may otherwise have pursuant to any State or federal law, regulation, or rule, to oppose any process employed by the Division to obtain such information, documents, or testimony.

11. NOTICES

11.1 Except as otherwise provided herein, any notices or other documents required to be sent to the Division or Diamond pursuant to this Consent Order shall be sent by United States mail, Certified Mail Return Receipt Requested, or other nationally recognized courier service that provides for tracking services and identification of the person signing for the documents. The notices and/or documents shall be sent to the following addresses and email addresses:

For the Division:

Cody I. Valdez, Deputy Attorney General
Office of the Attorney General
Department of Law and Public Safety
124 Halsey Street, 5th Floor
Newark, New Jersey 07101

Cody.Valdez@law.njoag.gov

For Diamond:

Anjali C. Das, Partner
Jennifer S. Stegmaier, Of Counsel
Wilson Elser Moskowitz Edelman & Dicker LLP
55 West Monroe Street, Suite 3800
Chicago, IL 60603

Anjali.Das@wilsonelser.com
Jennifer.Stegmaier@wilsonelser.com

IT IS ON THE 12th DAY OF October, 2021 SO ORDERED.

ANDREW J. BRUCK
ACTING ATTORNEY GENERAL OF NEW JERSEY

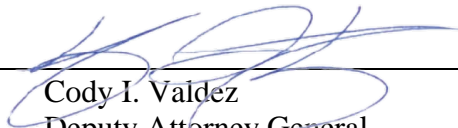
By: 
SEAN F. NEAFSY, ACTING DIRECTOR
DIVISION OF CONSUMER AFFAIRS

THE PARTIES CONSENT TO THE FORM, CONTENT AND ENTRY OF THIS CONSENT ORDER ON THE DATES ADJACENT TO THEIR RESPECTIVE SIGNATURES.

FOR THE DIVISION:

ANDREW J. BRUCK
ACTING ATTORNEY GENERAL OF NEW JERSEY

By: _____


Cody I. Valdez
Deputy Attorney General
124 Halsey Street, 5th Floor
Newark, New Jersey 07101

Dated: October 7, 2021

FOR DIAMOND INSTITUTE:



By: _____

Anjali C. Das
Wilson Elser Moskowitz Edelman & Dicker LLP
55 West Monroe Street, Suite 3800
Chicago, Illinois 60603

Dated: October 7, 2021