

ATTORNEY GENERAL OF THE STATE OF NEW YORK  
BUREAU OF INTERNET & TECHNOLOGY

---

In the Matter of

Assurance No. 23-052

**Investigation by LETITIA JAMES,  
Attorney General of the State of New York, of**

**US Radiology Specialists, Inc,**

Respondent.

---

**ASSURANCE OF DISCONTINUANCE**

The Office of the Attorney General of the State of New York (“NYAG”) commenced an investigation pursuant to, *inter alia*, Executive Law § 63(12) and General Business Law (“GBL”) §§ 349 and 899-bb into a data security incident at US Radiology Specialists, Inc. (“US Radiology” or “Respondent”). This Assurance of Discontinuance (“Assurance”) contains the findings of NYAG’s investigation and the relief agreed to by NYAG and US Radiology.

**NYAG FINDINGS**

1. US Radiology is one of the nation’s largest private radiology groups and provides managed services for several partner companies, including New York-based Windsong Radiology Group (“Windsong”).
2. Like other partner companies, Windsong relies on US Radiology for numerous services related to network management and protection.
3. To protect its networks and those of its partner companies from intrusion and other threats, US Radiology deployed a firewall sold by SonicWall.

4. On January 22, 2021, SonicWall published a product notification regarding a “coordinated attack on its internal systems” conducted by “highly sophisticated threat actors.” SonicWall believed the attackers had exploited “probable zero-day vulnerabilities” in specific SonicWall products used for remote access.

5. On January 31, 2021, researchers at NCC Group announce that they had identified a “possible candidate for the vulnerability” that SonicWall was investigating and three days later, SonicWall released a firmware patch to address the vulnerability.

6. Because its Sonicwall hardware was at an end-of-life stage and no longer supported with the latest firmware patch, US Radiology required a hardware replacement before it could install the firmware patch released by Sonicwall. US Radiology scheduled the hardware replacement project to take place in July 2021.

7. The hardware replacement project, however, was delayed due to competing priorities and resource restraints and the known vulnerability was not addressed as scheduled.

8. On December 8, 2021 a threat actor was able to gain access to US Radiology’s SonicWall with valid credentials. Once the threat actor gained access to the VPN, they leveraged 101 additional credentials to access various network data folders over the following week.

9. While a subsequent forensic investigation was unable to definitively determine how the threat actor initially obtained credentials to access the Sonicwall VPN, the vulnerability identified by the NCC Group in January 2021 could have allowed the threat actor to capture username, password and other session information stored on the SonicWall server through a process known as a SQL injection.

10. Because the threat actor obtained domain administrator and local administrator

account credentials and modify certain security protocols, the post-incident forensic investigation conducted by a third-party on behalf of US Radiology involved extensive analysis and was not completed until August 2022.

11. The forensic investigation ultimately concluded that the threat actor had been able to access protected health information (“PHI”), as defined by the Health Insurance Portability & Accountability Act (“HIPAA”), and private information (“PI”), as defined by New York’s breach notification law of 198,260 patients, including 92,540 Windsong patients that were residents of New York.

12. The PHI that was exposed during the incident included names, dates of birth, patient IDs, dates of service, provider names, types of radiology exams, diagnoses and/or health insurance ID numbers.

13. The PI that was exposed during the incident included names, driver’s license numbers, passport numbers, and Social Security numbers for 82,478 New Yorkers.

14. During the course of the forensic investigation, a cybersecurity firm hired by US Radiology engaged with the threat actor, who provided evidence of having possession of the exfiltrated data.

15. US Radiology concluded its review of documents exposed during the breach in August 2022 and, shortly thereafter, Windsong began mailing notification letters to individuals and, in accordance with HIPAA, posted substitute notice to its website and issued a press release to prominent outlets in New York, where applicable. US Radiology also offered one year of free credit monitoring to affected individuals.

16. The NYAG’s investigation determined US Radiology failed to adopt reasonable

data security practices to protect customer personal information by failing to protect the firewall from a known vulnerability.

17. Based on the foregoing, US Radiology violated Executive Law § 63(12), GBL §§ 349 and 899-bb.

18. Respondent neither admits nor denies NYAG's Findings, paragraphs 1-17 above.

19. The NYAG finds the relief and agreements contained in this Assurance appropriate and in the public interest. THEREFORE, the NYAG is willing to accept this Assurance pursuant to Executive Law § 63(15), in lieu of commencing a statutory proceeding for violations of Executive Law § 63(12) and GBL §§ 349 and 899-bb.

IT IS HEREBY UNDERSTOOD AND AGREED, by and between the Parties:

**PROSPECTIVE RELIEF**

20. For the purposes of this Assurance, the following definitions shall apply:

- A. "Effective Date" shall be the date of the last signature to this agreement.
- B. "Personal Information" shall mean information of New York residents defined as "private information" in GBL § 899-aa.
- C. "Security Event" shall mean any compromise that results in unauthorized access to or acquisition of Personal Information owned, licensed, or maintained by US Radiology.

**GENERAL COMPLIANCE**

21. US Radiology shall comply with Executive Law § 63(12), and GBL §§ 349 and 899-bb, as applicable, in connection with its collection, use, and maintenance of Personal Information, and shall maintain reasonable security policies and procedures designed to safeguard

Personal Information from unauthorized use or disclosure.

22. US Radiology shall not misrepresent the extent to which US Radiology maintains and protects the privacy, security, confidentiality, or integrity of Personal Information collected from or about customers.

### **INFORMATION SECURITY PROGRAM**

23. US Radiology shall enhance, implement, and maintain its existing written information security program (“Information Security Program”) that is reasonably designed to protect the security, integrity, and confidentiality of Personal Information that US Radiology collects, stores, transmits, and/or maintains. The Information Security Program shall, at a minimum, include the information security requirements set forth in this Assurance.

24. The Information Security Program shall comply with applicable data security requirements under New York state law, including General Business Law §§ 899-bb, and shall contain reasonable administrative, technical, and physical safeguards appropriate to: (i) the size and complexity of US Radiology’s operations; (ii) the nature and scope of US Radiology’s activities; and (iii) the sensitivity of the Personal Information that US Radiology collects, stores, transmits, and/or maintains.

25. US Radiology shall review the Information Security Program not less than annually and make any reasonable changes necessary to ensure the protection of the security, integrity, and confidentiality of Personal Information that US Radiology collects, stores, transmits, and/or maintains.

26. US Radiology shall appoint a qualified employee to be responsible for implementing, maintaining, and monitoring the Information Security Program with the credentials,

background, and expertise in information security appropriate to the level, size, and complexity of her/his role in implementing, maintaining, and monitoring the Information Security Program.

27. US Radiology shall provide notice of the requirements of this Assurance to its management-level employees responsible for implementing, maintaining, or monitoring the Information Security Program. US Radiology shall ensure that its executive IT leadership team and their direct reports are trained on the requirements of this Assurance within thirty (30) days of the Effective Date of this Assurance or prior to their responsibilities for implementing, maintaining, or monitoring the Information Security Program.

#### **PERSONAL INFORMATION SAFEGUARDS AND CONTROLS**

28. IT Infrastructure : US Radiology shall maintain, keep updated, and support critical IT assets on the US Radiology computer network to ensure that critical IT assets in the environment have not passed their end-of-life support and do not have known security vulnerabilities. At a minimum, US Radiology shall implement the following:

- a. End of Life: US Radiology shall create and implement a reasonable IT asset management program for identifying, reporting, and prioritizing and replacing or updating IT asset(s). For any hardware or software that will no longer be supported by the manufacturer or a third party, US Radiology shall commence the evaluation and planning to replace the IT asset(s) or to maintain the IT asset(s) with appropriate compensating controls at least two (2) years prior to the date on which the manufacturer's or third party's support will cease, or from the date the manufacturer or third party announces that it is no longer supporting the IT asset(s) if such period is less than two (2) years. If US Radiology is

unable to commence the evaluation and planning in the time frame required by this subparagraph, it shall prepare and maintain a written exception that shall include:

- i. A description of why the exception is appropriate, e.g., what business need, or circumstance supports the exception;
  - ii. An assessment of the potential risk posed by the exception; and
  - iii. A description of the schedule that will be used to evaluate and plan for the replacement of the IT asset(s) or addition of compensating controls.
- b. US Radiology shall maintain reasonable controls to address vulnerabilities and the potential impact security updates and security patches may have on the US Radiology computer network and shall:
- i. Maintain a reasonable patch management solution(s) to manage software patches by maintaining a database of patches; deploying patches to endpoints; verifying patch installation; and retaining patch history. When the security patch is released by the vendor the patch shall be deployed as quickly as possible for the affected IT asset(s).
  - ii. Maintain a process that includes an automated Common Vulnerabilities and Exposures (CVE) feed to keep track of potential security risks and to prioritize IT asset management of removal, replacement, or upgrade of the IT asset(s) in the environment.

29. Authentication Policy and Procedures: US Radiology shall implement and maintain a reasonable policy and supporting procedures implementing for account management and

authentication, including forbidding the use of shared user accounts, and requiring the use of multi-factor authentication for all Active Directory administrative or Virtual Private Network (“VPN”) remote access accounts. It shall be evaluated on an annual basis for ensuring its adequacy and relevancy regarding US Radiology’s needs and goals.

30. Encryption: US Radiology shall encrypt customer private information as defined by GBL § 899-aa(b) that it collects, stores, transmits and/or maintains, whether stored within the US Radiology computer network, or transmitted electronically within or outside the network, using a reasonable encryption algorithm.

31. Penetration Testing: US Radiology shall develop, implement, and maintain a penetration testing program designed to identify, assess, and remediate security vulnerabilities within the US Radiology computer network. This program shall include regular penetration testing, risk-based vulnerability ratings, and vulnerability remediation practices that are consistent with industry standards.

32. Logging and Monitoring: US Radiology shall implement and maintain an appropriate system designed to collect and monitor network activity, such as through the use of security and event management tools, as well as appropriate policies and procedures designed to properly configure such tools to report anomalous activity. The implemented system shall, at a minimum: (1) provide for centralized logging and monitoring that includes collection and aggregation of logging for US Radiology’s email systems, including logging all information security events detected; and (2) monitor for and alert security personnel to suspicious activity. Logs for network activity should be actively accessible for a period of at least 90 days and stored for at least one year from the date the activity was logged.



33. Data Deletion: US Radiology shall implement policies and procedures for permanently deleting customer Personal Information when there is no reasonable business purpose to retain it in accordance with applicable New York law.

34. US Radiology shall pay to the State of New York four hundred and fifty thousand Dollars (\$450,000), in civil penalties, attorneys' fees, and other costs of investigation (the "Monetary Relief Amount"). Payment of the Monetary Relief Amount shall be made in full within sixty (60) days of the Effective Date of this Assurance.

35. The Respondent shall provide NYAG with a certification affirming either its compliance with, or its target completion date(s) for its compliance with, the requirements set forth in this Assurance, paragraphs 23-33, to be submitted to NYAG within ninety (90) days of the Effective Date of this Assurance. This certification shall be in writing and be signed by an officer of Respondent. Thereafter, a certification of compliance shall be submitted to NYAG on an annual basis for the following two (2) years. In any case where the circumstances warrant, NYAG may require Respondent to file an interim certification of compliance upon thirty (30) days notice.

**MISCELLANEOUS**

36. Respondent expressly agrees and acknowledges that NYAG may initiate a subsequent investigation, civil action, or proceeding to enforce this Assurance, for violations of the Assurance, or if the Assurance is voided pursuant to paragraph 43, and agrees and acknowledges that in the event the Assurance is voided:

- a. any statute of limitations or other time-related defenses are tolled from and after the Effective Date of this Assurance;

b. the NYAG may use statements, documents or other materials produced or provided by Respondent prior to or after the Effective Date of this Assurance;

c. any civil action or proceeding must be adjudicated by the courts of the State of New York, and that Respondent irrevocably and unconditionally waives any objection based upon personal jurisdiction, inconvenient forum, or venue; and

d. evidence of a violation of this Assurance shall constitute prima facie proof of a violation of the applicable law pursuant to Executive Law § 63(15).

37. If a court of competent jurisdiction determines that Respondent has violated the Assurance, Respondent shall pay to the NYAG the reasonable cost, if any, of obtaining such determination and of enforcing this Assurance, including without limitation legal fees, expenses, and court costs.

38. This Assurance is not intended for use by any third party in any other proceeding.

39. All terms and conditions of this Assurance shall continue in full force and effect on any successor, assignee, or transferee of Respondent. Respondent shall include in any such successor, assignment or transfer agreement a provision that binds the successor, assignee or transferee to the terms of the Assurance. No party may assign, delegate, or otherwise transfer any of its rights or obligations under this Assurance without the prior written consent of NYAG.

40. Nothing contained herein shall be construed as to deprive any person of any private right under the law.

41. Any failure by the NYAG to insist upon the strict performance by Respondent of any of the provisions of this Assurance shall not be deemed a waiver of any of the provisions hereof, and the NYAG, notwithstanding that failure, shall have the right thereafter to insist upon

the strict performance of any and all of the provisions of this Assurance to be performed by Respondent.

42. All notices, reports, requests, and other communications pursuant to this Assurance must reference Assurance No. 23-052, and shall be in writing and shall, unless expressly provided otherwise herein, be given by hand delivery; express courier; or electronic mail at an address designated in writing by the recipient, followed by postage prepaid mail, and shall be addressed as follows:

If to Respondent, to:

US Radiology Specialists, Inc.  
700 East Morehead, Suite 300  
Charlotte, North Carolina 28202  
Attention: General Counsel

If to NYAG, to:

Bureau Chief  
Bureau of Internet & Technology  
28 Liberty Street  
New York, NY 10005

43. NYAG has agreed to the terms of this Assurance based on, among other things, the representations made to NYAG by Respondent and its counsel and NYAG's own factual investigation as set forth in NYAG's Findings, paragraphs 1-17 above. Respondent represents and warrants that neither it nor its counsel has made any material misrepresentations to NYAG. If any material misrepresentations by Respondent or its counsel are later found to have been made by NYAG, this Assurance is voidable by NYAG in its sole discretion.

44. No representation, inducement, promise, understanding, condition, or warranty not set forth in this Assurance has been made to or relied upon by Respondent in agreeing to this

Assurance.

45. Respondent represents and warrants, through the signature below, that the terms and conditions of this Assurance are duly approved.

46. Nothing in this Agreement shall relieve Respondent of other obligations imposed by any applicable state or federal law or regulation or other applicable law.

47. Nothing contained herein shall be construed to limit the remedies available to NYAG in the event that Respondent violates the Assurance after its Effective Date.

48. This Assurance may not be amended except by an instrument in writing signed on behalf of the Parties to this Assurance.

49. In the event that any one or more of the provisions contained in this Assurance shall for any reason be held by a court of competent jurisdiction to be invalid, illegal, or unenforceable in any respect, in the sole discretion of NYAG, such invalidity, illegality, or unenforceability shall not affect any other provision of this Assurance.

50. Respondent acknowledges that it has entered this Assurance freely and voluntarily and upon due deliberation with the advice of counsel.

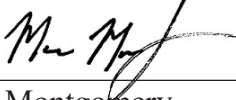
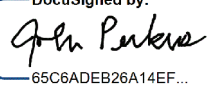
51. This Assurance shall be governed by the laws of the State of New York without regard to any conflict of laws principles.

52. The Assurance and all its terms shall be construed as if mutually drafted with no presumption of any type against any party that may be found to have been the drafter.

53. This Assurance may be executed in multiple counterparts by the Parties hereto. All counterparts so executed shall constitute one agreement binding upon all Parties, notwithstanding that all Parties are not signatories to the original or the same counterpart. Each counterpart shall

be deemed an original to this Assurance, all of which shall constitute one agreement to be valid as of the Effective Date of this Assurance. For purposes of this Assurance, copies of signatures shall be treated the same as originals.

WHEREFORE, THE SIGNATURES EVIDENCING ASSENT TO THIS Assurance have been affixed hereto on the dates set forth below.

<p><b>LETITIA JAMES</b> <b>ATTORNEY GENERAL OF THE</b> <b>STATE OF NEW YORK</b></p> <p>By:  _____ Marc Montgomery Assistant Attorney General Bureau of Internet and Technology New York State Attorney General 28 Liberty St. New York, NY 10005</p> <p>11/2/2023 _____ Date</p>	<p><b>US RADIOLOGY SPECIALISTS, INC.</b></p> <p>DocuSigned by:  65C6ADEB26A14EF...</p> <p>By: _____ John Perkins CEO/President US Radiology Specialists 4200 Six Forks Road, Suite 1000 Raleigh, NC 27609</p> <p>10/31/2023 _____ Date</p>
---	--