NUANCE COMMUNICATIONS, INC. ONE WAYSIDE ROAD BURLINGTON, MA 01803 781 565 5000 NUANCE.COM

NUANCE

July 25, 2017

Dear Valued Healthcare Customer:

As you are aware from our prior communications (including notice on our website, daily calls, contact from customer service representatives, and other communications to you), Nuance Communications, Inc. ("*Nuance*") was impacted by a global malware incident that affected certain of our systems—including certain systems that store or transmit protected health information ("*PHI*"). This communication is intended to provide you with a further update on the incident and Nuance's response effort, as well as to share the working conclusions Nuance has reached with respect to how this incident is appropriately characterized for purposes of HIPAA. This communication, along with those we have previously provided to you, is part of Nuance's ongoing effort to ensure that, to the extent Nuance is your business associate for purposes of HIPAA, we fulfill our obligations under our Business Associate Agreement ("*BAA*") with you. All facts and conclusions that we communicate here are based upon the information known to Nuance to date, and are subject to revision to the extent any new information subsequently comes to light that necessitates such revision (in which case we will notify you).

What Happened

Beginning approximately 7:00 am Eastern Time on June 27, 2017, Nuance was a victim of a crime: the global NotPetya malware incident (the "*Incident*"). The NotPetya malware affected certain Nuance systems[1], including Nuance systems on which files containing electronic protected health information ("*ePHI*") are stored and/or transmitted. The information available to Nuance about the NotPetya attacks, including information from the U.S. Department of Homeland Security's U.S. Computer Emergency Readiness Team ("*US-CERT*"), other relevant U.S. government agencies, and other reputable sources, indicates that:

- Despite media reports to the contrary, the NotPetya malware actually was not ransomware. It was not designed to give its perpetrator(s) any capability to control data on affected systems. To date, we have seen no indication that the malware functioned differently in practice on affected Nuance systems.

- The malware was not designed to allow any unauthorized party to view any file contents (including ePHI) on affected systems, nor have we seen any indication that it actually functioned in that manner on affected Nuance systems.

- The malware was not designed to copy or extract any file contents (including ePHI) from affected systems or to give its perpetrator(s) any capability to control data on affected

[1] For the purposes of this document, "systems" means Nuance-owned and operated servers, desktops, and laptops.

systems. To date, we have seen no indication that the malware functioned to do any of these things in practice on affected Nuance systems.

- The malware was not designed to target the types of files in which Nuance stores ePHI and we have seen no evidence that those file types actually were targeted in this Incident.

Based on those key facts, Nuance has concluded that:

1. The Incident constitutes a "security incident" for purposes of the HIPAA Security Rule because it involved "the *attempted* or successful unauthorized… modification, or destruction of information or interference with system operations in an information system."[2] [emphasis added.]

2. There is no evidence that any PHI was acquired, accessed, used, or disclosed in an unauthorized manner that compromised the privacy or security of the PHI and, therefore, the Incident does not fall within the definition of a presumptive breach of unsecured PHI for purposes of the HIPAA Breach Notification Rule ("*BNR*")[3];

3. Even if the Incident met the definition of a presumptive breach, it would fall within a specific exclusion under the BNR because Nuance believes in good faith, and with good reason, that no unauthorized person reasonably could have retained any PHI (because there is no indication that any PHI was viewed, extracted, or copied by any unauthorized person in the first place)[4]; and

4. Even if the Incident met the definition of a presumptive breach and did not fall within a specific exclusion under the BNR, the four-factor test set forth as part of the BNR's definition of "breach" has led Nuance to conclude in good faith that there is a low probability that any PHI was compromised during the Incident for purposes of HIPAA and the BNR.[5]

Accordingly, based on facts presently known, while Nuance has determined that the Incident constitutes a security incident for purposes of the HIPAA Security Rule, Nuance also has determined the Incident does not constitute a breach of unsecured PHI for purposes of the BNR.[6] Nuance is keeping you advised of the Incident and its response effort as a courtesy and to fulfill any BAA obligations Nuance may have to you to provide notice in the event of a security incident.

---

[2] See 45 C.F.R. § 164.304.
[3] See 45 C.F.R. § 164.402.
[4] See 45 C.F.R. § 164.402(1)(iii).
[5] See 45 C.F.R. § 164.402(2).
[6] The U.S. Department of Health and Human Services ("*HHS*"), which administers and enforces HIPAA, has explicitly acknowledged that a "security incident" for purposes of the HIPAA Security Rule does not necessarily constitute a "breach" for purposes of the BNR. See, e.g., 78 Fed. Reg. 5656-5657 (Jan. 25, 2013).

What Steps We Have Taken

While we do not believe this Incident constitutes a breach under HIPAA, Nuance took immediate action to ensure that the Incident was contained and any impacts mitigated to the extent reasonably possible. As a precautionary measure, we shut down our networks, transcription platforms, and other systems to halt the potential spread of the malware. We have been conducting an extensive, around the clock, systems evaluation and restoration effort utilizing external consultants and our internal IT teams.

Pursuant to our internal incident response policies and published guidance from HHS, we established contact with the local Federal Bureau of Investigation ("*FBI*") field office and The U.S. Department of Homeland Security ("*DHS*"). DHS has confirmed to us that, similar to our own experience, other entities affected by this global malware incident did not experience any exfiltration or acquisition of their data.

We continue to work with customers to restore and reestablish access to any PHI from affected Nuance systems that customers need.

Our focus and priority is to maintain the security and safety of the systems and data, so we are being cautious on the pace of redeployment.

Additional Information

We have established a website that is updated regularly to keep customers informed on this matter. The website can be accessed at: https://www.nuance.com/healthcare/customer-update.html. We encourage you to check this website frequently for updates. You may also contact your Nuance customer service representative for additional information.

Nuance continues to take the privacy and security of all confidential information you entrust to us very seriously. If you have any questions about this Incident, our working conclusions summarized above, or our ongoing remediation steps, please do not hesitate to contact your Account Representative

Sincerely,

Nuance Communications, Inc.