Dated: January 20, 2013 *Tejaswi Worlikar*

To,
The Management,
Mix-All-The-Compounds Inc.
Y U No Mix Parkway
Ann Arbor,
MI 48109-2121 USA.

Subject: Recommendations for drafted response to FDA regarding MedWatch 3500 form

Dear Sir,

It is unfortunate to learn of the MedWatch 3500 filed against our device Ther-Mix-A-Lot-25 and the ensuing adverse event reporting in MAUDE. It is imperative that we take necessary measures to minimize the damage not only to the reputation of our device in the market, but the stock of our company as whole.

Keeping that in mind, I would like to propose certain amendments to the text in the FDA response draft. The text, *"Any changes to the original, validated image, including installation of antivirus software, nullifies the validated state, may create an unsafe operating condition, and would constitute off-label use. In addition, our company does not regularly install operating system updates or patches for this device",* might be interpreted by FDA and the customers as a violation of the FDA guidelines. There are multiple guidance documents and I will summarize the relevant directives here (I have attached the full list for detailed references). The FDA Guidance document titled '**Reminder from FDA: Cybersecurity for Networked Medical Devices is a Shared Responsibility'** dated November 4, 2009**,** clearly states that both the manufacturer and the customer are responsible for safe use of the device, and that typically, software changes for security enhancements do not need FDA approval. Furthermore, an older FDA document '**Guidance for Industry - Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software',** dated January 14, 2005**,** deems that the device manufacturer using OTS software (in this case, Doors XP) bears the responsibility for the continued safe and effective performance of the medical device ***and*** the performance of the OTS software that is part of the device.

However the solution is not as ingenuous as updating the software, because under sections 21 CFR 820.100, 21 CFR 820.30(g) and 21 CFR 820.30(i), as manufacturers, it is our prerogative to identify cyber-security vulnerabilities and any software changes to address these are classified as design changes and require validation according to the established protocol. And as you are aware, since this requires massive investment of time and labor, it has not been our policy to support software changes. Taking into account the best interests of the company vis-à-vis FDA as well as customer satisfaction and patient safety, I recommend some alternatives.

I would advise you to delete the comment '*In addition, our company does not regularly install operating system updates or patches for this device'* and instead use '*Our company provides warranty to devices operating **only** in the original validated state, and this state can be safeguarded by faithfully following our product security guidelines. To summarize here, the customer is specifically instructed to do so by isolating the device from the network using a dedicated firewall or other external means, and **not** installing any security software on the machine itself'.* And as a secondary measure, I sincerely urge you to consider revising our existing policies to extend security support to our devices in the future. It is crucial that we recognize this incident not as a stray, but as an indication of the times we live in. Security from malicious software attacks is just as grave in medical equipment as it is in the IT sector, perhaps more so; the issue goes beyond any particular company or device because lives are at stake. And therefore, the hospitals' concerns are justified. Mitigating them is not only our business commitment, but also in a way, our corporate social responsibility.

Having underlined the magnitude and implications of the situation, I suggest you amend the draft to the FDA. I also request you to appreciate the broader picture in terms of foreseeable and avertable security risks, and take urgent proactive steps to prevent such adverse reporting events in the future.

Yours sincerely,

A.B.C
Product Manager - Ther-Mix-A-Lot-25,
Mix-All-The-Compounds Inc.

REFERENCES:

1. Information for Healthcare Organizations about FDA's "Guidance for Industry: Cybersecurity for Networked Medical Devices Containing Off-The-Shelf (OTS) Software" *http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm070634.htm*
2. Guidance for Industry, FDA Reviewers and Compliance on Off-The-Shelf Software Use in Medical Devices
   http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm073778.htm
3. Reminder from FDA: Cybersecurity for Networked Medical Devices is a Shared Responsibility *http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm189111.htm*
4. Guidance for Industry - Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software
   http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077812.htm
5. Preventing Cyber Attacks, Baxa Corporation
   https://btsp.baxa.com/Sales%20Portal/ExactaMix/Preventing%20Cyber%20Attacks.pdf
6. MAUDE Adverse Event Report: BAXA CORP.EXACTA-MIX 2400 *http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfMAUDE/detail.cfm?mdrfoi__id=1719489*
7. MAUDE Adverse Event Report: BAXA CORPORATIONBAXA EM2400 COMPOUNDER *http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfMAUDE/detail.cfm?mdrfoi__id=1621627*