ACUPUNCTURE Today


YOUR PRACTICE / BUSINESS

# Avoiding the Perils of Data Breaches

## RED FLAGS: CLOUD-BASED MARKETING / EMAIL SERVICES

David Bibbey, Dipl. Ac., LAc

### WHAT YOU NEED TO KNOW

- Mailchimp announced on its website earlier this year that it identified a hacker had accessed its system, exposing customer data.
- This highlights the importance of acupuncturists understanding and following HIPAA privacy & security rules.
- Other companies offering similar services should be evaluated for their HIPAA compliance, like Constant Contact, Zoho Campaigns, Drip, MailerLite, Campaigner, GetResponse, and Moosend.

*Editor's Note:* This is the latest in an ongoing series devoted to assisting acupuncture practitioners in understanding and complying with different aspects of the Health Insurance Portability and Accountability Act (HIPAA). The first article appeared in February 2022.

---

Mailchimp [a marketing automation and email marketing platform used by many health care providers] announced on its website earlier this year that it identified a hacker had accessed its system, exposing customer data. (This was the company's second hacking event in six months.) Mailchimp was first breached in April 2022, and hackers were able to view around 300 user accounts, stealing data from 102 of them. As a result, the affected health care businesses were warned about potential email phishing attacks targeting their clinics and patients.

Health care clinics and marketing groups working with Mailchimp confirmed that clients had been affected by malicious password resets, and last December 2022, it was reported that "API keys" for Mailchimp had been leaked, potentially allowing hackers access to email conversations and potentially sensitive information. API stands for "application programming interface" and is used

for software applications to send and receive data.

An API key leak allows hackers actor to read conversations, copy customer information, expose email lists of multiple campaigns containing PII and PHI [personally identifiable information and protected health information], authorize third-party applications connected to a Mailchimp account, manipulate promo codes, and start a fake campaign and send emails posing to come from an acupuncturist's office.

Relevance to Your Practice

All this highlights the importance of acupuncturists understanding and following HIPAA privacy & security rules; in particular, the requirements for having any outside vendor that handles or manages patients' PHI sign a business associate agreement (BAA) and for them to be HIPAA compliant.

Mailchimp does not sign a BAA for covered entities (health care providers). Why? Because the company does not provide HIPAA-compliant email marketing services. Mailchimp provides reliable services that successfully meet the needs of lots of businesses, but *not* for health care providers who have to comply with HIPAA patient privacy and data security rules.  A review of Mailchimp's Terms of Use reveals it clearly states:

*#20 Compliance with Laws: You represent and warrant that your use of Mailchimp will comply with all applicable laws and regulations. You're responsible for determining whether our Services are suitable for you to use in light of any regulations like HIPAA, GLB, EU Data Privacy Laws, or other laws. If you're subject to regulations (like HIPAA) and you use our Service, then we won't be liable if our Service doesn't meet those requirements.*

For acupuncturists who share or store names, email addresses, and additional patient data in a cloud-based marketing service like Mailchimp, HIPAA requires that all of the data is stored securely and that the vendor is HIPAA compliant.

Remember that any marketing or other email you send to patients contains both their name and an email address in the header, so really, you can't send any emails via Mailchimp in a HIPAA-compliant manner. If the vendor isn't able (or willing) to sign a BAA, it puts health care businesses in a vulnerable position. This should be a red flag for clinic owners and managers.

Although Mailchimp is referenced here because of its recent data breach notifications, other companies offering similar services should be evaluated for their HIPAA compliance, like Constant Contact, Zoho Campaigns, Drip, MailerLite, Campaigner, GetResponse, and Moosend.

---

*Author's Note:* For more information, please visit www.patientdataprotection.com or call Matthew Fiorenza, compliance and security specialist, at 352-268-5088, ext. 4.

JULY 2023