HIPAA

Compliant Bulk Emailing Basics

A Technical Guide to Bulk Emailing

by Erik Kangas, PhD

LUXSCI

www.luxsci.com

TABLE OF CONTENTS

INTRODUCTION

Are my emails reaching my intended audience? That's a question every email marketer has asked themselves at some point. The way to measure your success in getting emails into users' inboxes is through deliverability, and "high deliverability" is the key to effective bulk emailing. Whether you're sending out the latest coupons or details about an upcoming event, you need to know that your promotional materials are getting through to the people who will enjoy or draw value from them. But ensuring high deliverability takes some expertise.

This technical guide by LuxSci provides marketers and business owners like you with the tips and tools necessary to optimize the deliverability of your email messages. From blacklist prevention to IP reputation management, applying LuxSci's knowledge about bulk emailing will help set your campaigns up for success. And for those of you who work in healthcare, Chapter 5 talks specifically about the additional best practices you must follow to abide by the Health Insurance Portability and Accountability Act (HIPAA).

CHAPTER 1

List Maintenance Best Practices

Deliverability begins with proper list maintenance. There's no point in sending messages to recipients who no longer exist or, even worse, don't want to receive them. Email lists should only contain recipients who've explicitly opted in, meaning that the recipient has actively and knowingly chosen to become a member of your mailing list.

Companies are also required to follow the CAN-SPAM Act[1] , the law that outlines how commercial emails need to be handled regarding recipient opt-ins and opt-outs. Finally, companies need to follow their email provider's terms of service. Failure to do so can result in you being blacklisted or having your account removed altogether.

Though keeping up with these regulations may seem like a daunting task, it's one that will make the difference between a successful email marketing campaign and one that falls flat on its face. The following list maintenance best practices will help make the bulk emailing business that much easier.

- **Remove Unnecessary Emails**
  Addresses that are invalid, fail to deliver, or are non-functional need to be purged from your mailing list. Many email providers monitor how many emails are sent to invalid addresses. Sending too many of these messages could result in your emails being temporarily or permanently blocked, as this is indicative of a poor quality list (e.g., purchased or scraped from websites).

- **Remove Recipients Who've Marked You as Spam**
  If you're able, try to find and remove any email recipients who've marked your emails as spam. Many people don't use opt-out or unsubscribe requests out of laziness or for fear that confirming their address will result in more emails; instead, they mark you as spam. Cleaning your lists of these emails reduces your chances of being reported to email providers.

- **Remove Opt-out Recipients**
  Remove all people who've requested to opt-out of your mailing list. The CAN-SPAM Act requires companies to honor all recipient removal requests. Failure to do so can result in the recipient reporting you to their email provider, leading to a potential blacklisting.

CHAPTER 2

Large-scale Sending Strategies

Once your email lists are cleaned up, it's time to focus on finding the best strategy for sending your large-scale campaigns.

Separate Business and Marketing Emails

Business and marketing emails serve two distinct purposes. Business emails (also known as transactional emails) are sent by billing, support, and other departments. They're typically sent on an individual basis and help maintain customer relationships. Marketing emails are usually sent in bulk and include newsletters, promotions, and blog/company updates. These differences present an issue when it comes to deliverability.

Marketing emails, by their very nature, are likely to bother some recipients because they're focused on promoting your company. If recipients report you or mark your promotional emails as spam, that could affect the deliverability of every other email sent from the same server or domain. To avoid damaging the communication that needs to happen with your customers, send out your transactional and marketing emails from separate servers or even different domains.

- **Use a Dedicated Server**
  A dedicated server meets these two criteria: You own the server and its resources, meaning you're not sharing the server with anyone else. This allows for faster email delivery times, as sharing server resources can result in slower performance.

- The server has a dedicated IP address that's also yours. Internet service providers (ISPs) look at the reputation of IP addresses when determining the deliverability of your messages. Having your own address means you're in complete control of your reputation. Sharing an IP address opens you up to reputation damage if another user is violating acceptable use policies set by the service provider.

Use Multiple Servers

Multiple servers can benefit companies in two ways:

- **Speed and volume:**
  Servers have a limit to the number of messages they can process at once. Having more than one dedicated server may be worth the investment if you're sending massive amounts of emails (e.g. 100K+ emails per day or 10K+ per hour). Multiple servers also give you the flexibility to set up and take down servers according to fluctuations in your business (e.g., higher volumes during the holidays).

- **Failover and reputation:**
  Having multiple servers provides you with a backup solution for sending emails in case one server fails. Regarding reputation, multiple servers with different IP addresses prevent one server from becoming suspect by ISPs due to high sending volumes.

CHAPTER 3

IP Reputation Challenges

IP reputation management directly impacts the deliverability of your emails. Focus on the eight critical factors below to improve your reputation and ensure better deliverability.

- **Number of messages sent from your server**
  Servers that suddenly blast out heavy volumes of emails risk being flagged and, as a result, may be blacklisted or taken down. Start out by sending small email blasts of no more than a few thousand at a time. Over a few weeks, you can slowly increase your volume amount. This gives ISPs time to recognize your IP address and understand it's not being used to send out spam messages.

- **Number of messages marked as spam by recipients**
  IP reputation can be affected by the number of recipients who mark your emails as spam. Marketers should subscribe to feedback loops (a service some mailing services already provide), which send notifications when someone marks an email as spam. Marketers can easily remove these addresses from their mailing lists and avoid having their IP reputation take a hit.

- **Sending frequency to invalid addresses**
  An email blast sent to a high number of invalid addresses is a sign of a poor quality list, which can damage your IP reputation. Pay close attention to email bounce rates and immediately remove all addresses that can't be delivered.

- **Message delivery rate**
  Some ISPs only allow a certain number of emails to be delivered from one IP address at a given time, and going beyond these limits can lead to a blacklisting. Avoid this by either sending your messages at slower rates or by spreading out deliveries across multiple servers with unique IP addresses.

- **Your IP address present on any blacklists**
  You can check MXToolbox2 to see if you're on any common blacklists. If your server is blacklisted, work with providers to get your server removed and find out what behavior caused the listing so you can avoid future hassle.

- **Proper IP address setup**
  Your IP should be static, not be owned by an ISP (e.g., Comcast, Verizon) and not be in a public cloud (e.g., Amazon, Rackspace). ISP and cloud IPs are easily and commonly used by spammers and thus constitute a "bad neighborhood" that will impact your deliverability.

- **Who else is sending emails from your IP address**
  Having your own server prevents other parties from sending emails from your IP address. This is important because if another company sharing your IP address starts sending spam, your reputation will suffer.

- **IP legacy**
  It's possible that another company used your IP address before it was assigned to your server. If that use created a poor reputation, it will transfer over to you even though you're just inheriting the address! In this case, you should work to get your IP address removed from blacklists, wait a few weeks before sending your own emails, or start off by sending small batches with friendly messaging to reliable lists. (Of course, you can also get a new IP address, too.)

CHAPTER 4

SPF and DKIM Considerations

ISPs take several factors into account when determining if your messages should be delivered to your recipients — including IP reputation and email content. Internet spam can sometimes sneak into recipients' inboxes through forged email addresses. For this reason, ISPs value senders who provide a means to validate their authenticity.

Setting up Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM) enable recipient servers to check if the email coming from your domain is legitimate or forged. This makes it easier for ISPs to validate your domain's identity and increases the deliverability of your messages. Marketers should turn to their email service provider for guidance on how to get these set up.

CHAPTER 5

HIPAA-compliance Specific

In addition to all the best practices for traditional email marketing, those of you working in the healthcare industry have other regulations to keep in mind. The Health Insurance Portability and Accountability Act (HIPAA)3 lays out standards for protecting patient data and privacy. Take note of the following points to certify that your bulk emailing is HIPAA-compliant.

Understand ePHI

Protected Health Information (PHI) and its electronic cousin (ePHI) consist of two parts: protected health information and information that personally identifies a patient. Examples of this include patient files that contain names and health history or simple appointment reminder emails that contain a patient's name and email address. HIPAA requirements state that all PHI and ePHI must be kept secure and protected.

Despite these seemingly straightforward definitions, there are many ambiguities to PHI. For instance, a patient's email address that doesn't include their name is still considered identifiable because the email can be traced back to the individual.

Another example is a newsletter that contains various healthcare tips and is sent to a subscriber list. If you work for a general health site that provides tips across different areas of health and fitness, ePHI doesn't likely apply. If your tips are related to the specific medical procedures practiced by your doctors and the list is a list of current, former, or future patients, then the messages may be ePHI and HIPAA may apply.

Healthcare marketers need to understand these nuances. For those new to the field, you might consider taking a class or hiring a consultant. For those well-versed in HIPAA-compliance, continued training and refreshers never hurt!

HIPAA Privacy Rule

Among the HIPAA guidelines is the Privacy Rule[4], which mandates that individuals must give written approval before their PHI can be used for marketing purposes. Marketing falls under two broad definitions:

Communications about products or services that encourage recipients to purchase said products. The disclosure of patient information from one entity to another to the benefit of the recipient party. For example, a health insurance company selling member information to a company that sells medical equipment in the hopes members will purchase said equipment.

Healthcare marketers need to know if they've received authorization from patients before including them on email lists, usually by having them complete the 45 CFR 164.508 form[5].

Understanding the Business Associates Agreement (BAA)

Given the importance of the compliance regulations set by HIPAA, healthcare organizations need to know that their email providers understand them as well. Healthcare marketers must get their email providers and any other vendors that handle their ePHI to sign a Business Associate Agreement (BAA) that includes HIPAA provisions[6].

The agreement lays out how the third party (e.g., email service provider) will protect and handle ePHI. In the event of a breach, the BAA also explains which entity is responsible for correcting the breach — typically the customer of the business associate is responsible for reporting it, and the organization that caused it is responsible for the fix. If your current or potential email provider is unfamiliar with HIPAA-compliance, you need to note the danger of that and seriously consider switching.

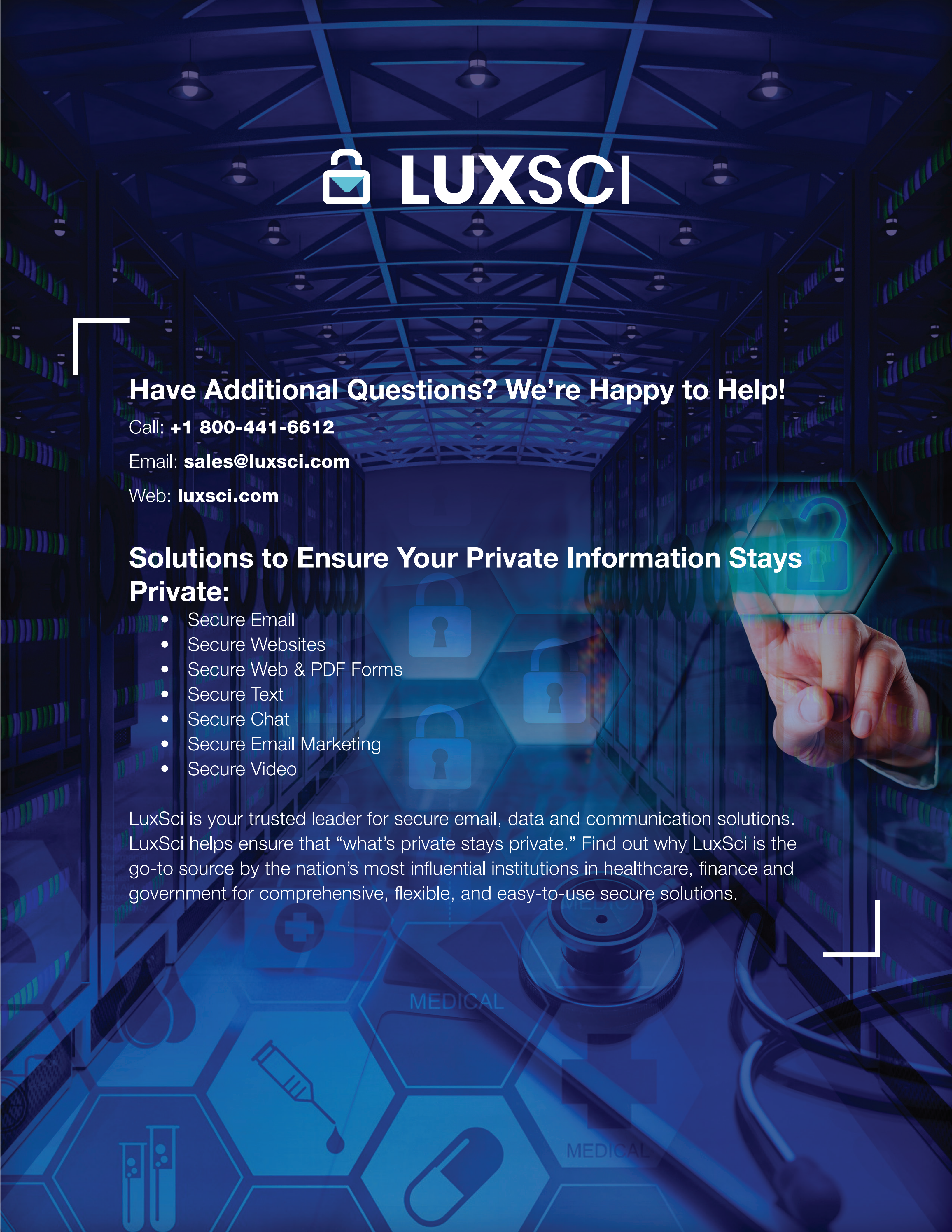
Making the Most of Your Bulk Emailing Strategy

There's a lot of nuance and strategy involved with bulk emailing and deliverability. ISPs, email providers, and government regulations can all influence the content and frequency of your messaging. Balancing factors like speed while maintaining a good reputation is what separates good email marketers from the great ones.

No email marketer starts out alone. Turn to your team for help in maintaining your email lists. Seek out experts in regulated or complex industries like healthcare. Find an email provider that understands reputation management and can make recommendations for server use. Once you're equipped with the knowledge that goes into creating a solid bulk email strategy, you're ready to get started. Higher deliverability awaits!

SOURCES:

http://mxtoolbox.com/blacklists.aspx
https://mailchimp.com/about/deliverability/
http://luxsci.com/blog/hipaa-compliant-email-marketing.html
http://www.pacortho.org/pdf/medical-records-release-form.pdf
http://luxsci.com/blog/hipaa-compliant-email-marketing-2.html
https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/marketing/
https://luxsci.com/blog/sharing-patient-list-marketing-company-ok-hipaa.html
https://luxsci.com/blog/high-volume-bulk-email-key-ingredients-for-good-deliverability.html
https://luxsci.com/blog/case-study-securely-send-medical-laboratory-results-to-patients.html
https://luxsci.com/blog/hipaa-compliance-is-needed-for-emailed-appointment-reminders.html
https://www.ftc.gov/tips-advice/business-center/guidance/can-spam-act-compliance-guide-business
https://luxsci.com/blog/maximizing-delivery-speed-and-reliability-for-large-scale-email-marketing.html
https://luxsci.com/blog/8-factors-governing-ip-reputation-increasing-email-marketing-deliverability.html
https://luxsci.com/blog/why-you-should-separate-your-business-and-your-marketing-email-sending.html
https://luxsci.com/blog/what-exactly-is-ephi-who-has-to-worry-about-it-where-can-it-be-safely-located.html



LUXSCI

Have Additional Questions? We’re Happy to Help!

Call: **+1 800-441-6612**

Email: **sales@luxsci.com**

Web: **luxsci.com**

Solutions to Ensure Your Private Information Stays Private:

- Secure Email
- Secure Websites
- Secure Web & PDF Forms
- Secure Text
- Secure Chat
- Secure Email Marketing
- Secure Video

LuxSci is your trusted leader for secure email, data and communication solutions. LuxSci helps ensure that “what’s private stays private.” Find out why LuxSci is the go-to source by the nation’s most influential institutions in healthcare, finance and government for comprehensive, flexible, and easy-to-use secure solutions.