HIPAA

Compliant Email Basics

Safeguarding Your Healthcare Practice and Protecting Patient Privacy

by Erik Kangas, PhD

LUXSCI
www.luxsci.com

TABLE OF CONTENTS

INTRODUCTION

Since the 1990s, the healthcare industry has benefited enormously from the many advances in technology made possible by the Internet. In the quest to integrate individual medical information from a variety of sources, the “digital revolution” has had a profound effect on patient care delivery. Now, patient information can be stored, appointments can be scheduled, data can be shared among medical providers, and appropriate medical services can be implemented.

The endurance of the Hippocratic Oath, dating from 400 BC, recognizes the essential, and even sacred, nature of patient confidentiality to the practice of medicine. One of the health care industry’s greatest challenges today is to ensure such confidentiality in the face of government regulation. Non-profit organizations and businesses alike must take adequate measures to safeguard the electronic communication of patient information.

This LuxSci eBook is your well-researched guide to both a critical understanding of the specific issues and concepts of HIPAA, HITECH, and the Omnibus rule, and their practical application to your business, so that you stay compliant with these government standards. This document will provide a framework for your health care entity to keep the privacy of patient information front and center. Providers will have the necessary tools to meet all requirements established by HIPAA to access email outsourcing services, as expertly configured by LuxSci.

CHAPTER 1

Overview of HIPAA

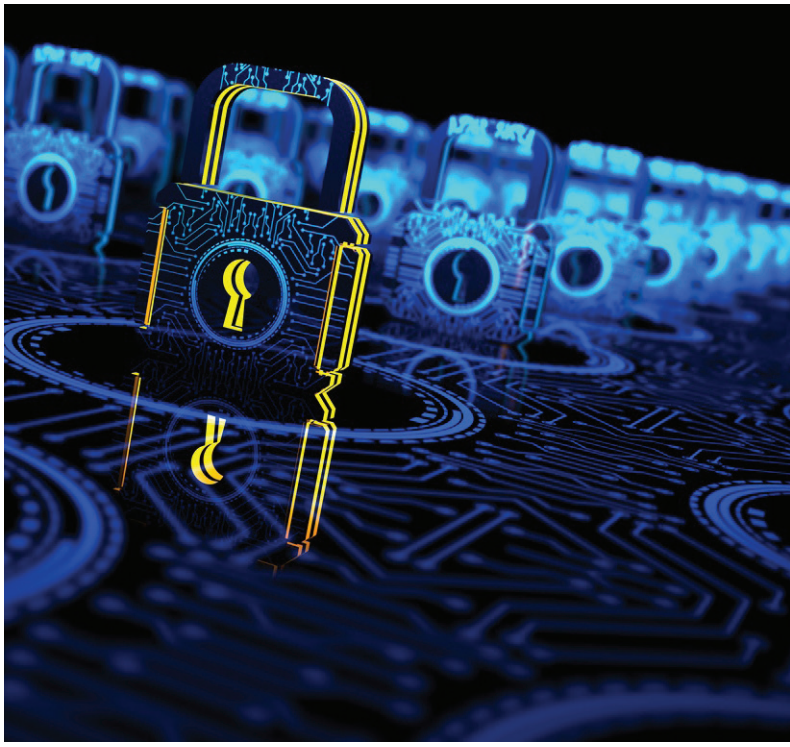
The Health Insurance Portability and Accountability Act of 1996 (HIPAA) devised a comprehensive set of rules regarding privacy and security to be adhered to by all sectors of the health care industry. While industry professionals - financial, administrative, and clinical - were no strangers to a regulatory compliance culture, HIPAA laws applied to "**Covered Entities**," - health care providers, clearinghouses, and health plan payers that met certain criteria.

Most providers, in fact, were considered covered entities if they maintained an electronic-based office - meaning they functioned by storing and exchanging data via intranets, the Internet, dial up modems, DSL lines, T-1 lines, and the like. Additionally, the 2009 Healthcare Information Technology for Economic and Clinic Health Act, better known as HITECH, and the Omnibus rule - the 2013 amended HIPAA Act - extended the requirements of HIPAA to any "**Business Associate**" of a covered entity and to all **Business Associates of Business Associates** (all the way down the line) that might come into contact with Protected Health Information (PHI) originating from a covered entity.

Electronic Protected Health Information (ePHI), as defined in HIPAA language, is health information of an identifiable individual that is transmitted by electronic media; maintained in any electronic medium; or transmitted or maintained in any other form or medium. For example, all administrative, financial, and clinical information on a patient is considered PHI.

The Privacy and Security Rules focus on information safeguards and require Covered Entities and their Business Associates to implement the necessary and appropriate means to secure and protect health data. Specifically, the regulations call for for organizational and administrative requirements along with technical and physical safeguards.

Starting in February 2010, the HIPAA rules were enhanced by the American Recovery and Reinvestment Act. The HITECH section of this act implements significant penalties for breaches of HIPAA and requires that the business partners of organizations covered by HIPAA must themselves obey the HIPAA Privacy and Security Rules, and face liability if there are any unauthorized disclosures.



Privacy Standards:
The HIPAA Privacy Rule sets standards for protecting the rights of individuals (patients). Covered Entities must follow the laws that grant every individual the right to the privacy and confidentiality of their health information. Protected Health Information is subject to an individual's rights on how such information is used or disclosed.

Privacy Standard Key Point:
Controlling the use and disclosure of oral, written, and electronic protected health information (any form).

Security Standards:
Taking the Privacy Rule a step further, HIPAA implemented the Security Rule to cover electronic PHI (ePHI). To this end, more secure and reliable information systems help protect health data from being "lost" or accessed by unauthorized users.

Security Standard Key Point:
Controlling the access to electronic forms of protected health information (not specific to oral or written).

CHAPTER 2

What is ePHI?

The phrase “electronic protected health information” (ePHI) often generates confusion and misinformation about exactly what ePHI is. Federal regulations, as established by the HIPAA Privacy Rule, protect health information that is produced, stored, transferred, or received in an electronic format against unauthorized use and disclosure. That is the crux of ePHI

A total of 18 “individually identifiable” factors can link health information to a specific individual, regardless of whether they are direct - such as name, address, social security number - or indirect, such as an obscure email address, account number, or IP address. Protected health information refers specifically to three classes of patient data, together with one or more factors that make it identifiable. These classes include information about the past, present, or future:

1. **Physical or mental health condition**
2. **Provisioning of health care (e.g. appointments)**
3. **Payment-related information for the provisioning of said health care**

The HIPAA Security Rule mandates that health data already in existence, or generated in the future, be protected as ePHI, by the following individuals, organizations, and agencies:

Covered Entities According to HIPAA

1. Health Care. A provider of services or supplies related to the physical or mental health of an individual. This includes: (1) preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling; service, assessment, or procedure with respect to the physical or mental condition or functional status of an individual or that affects the structure or function of the body; and (2) the sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.

2. Health Care Provider. A provider of services (as defined in section 1861(u) of the Act, 42 U.S.C. 1395x(u)), a provider of medical or health services (as defined in section 1861(s) of the Act, 42 U.S.C. 1395x(s)), and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.

3. Health Care Clearinghouse. A public or private entity – including a billing service, repricing company, community health management information system, or community health information system, and "value added" networks and switches – that (1) either processes or facilitates the processing of health information received from another entity in a non-standard format or containing non-standard data content into standard data elements or a standard transaction, or (2) receives a standard transaction from another entity and processes or facilitates the processing of health information into a nonstandard format or nonstandard data content for the receiving entity.

4. Health Plan. With certain exceptions, an individual or group plan that provides or pays the cost of medical care (as defined in section 2791(a)(2) of the Public Health Service PHS Act, 42 U.S.C. 300gg-91(a)(2)). The PHS law specifically includes many types of organizations and government programs as health plans.

Business Associate of a HIPAA Covered Entity

An individual or entity that performs certain functions or activities that involve the use or disclosure of ePHI on behalf of, or provides services to a covered entity. A member of a covered entity's workforce is not a business associate.

Business Associate of a Business Associate

A subcontractor that creates, receives, maintains, or transmits ePHI on behalf of another business associate. A business associate of a business associate is held to the same legal liability requirements as the primary HIPAA business associate.

CHAPTER 3

Provisions of the HIPAA Email Security Rule

The terminology of HIPAA uses the terms "required" and "addressable". These are actually easy-to-understand and discrete references.

Required: compliance with the given standard is mandatory. If your organization deals with any electronic communications that may be subject to HIPAA regulations, then it is incumbent on you to scrutinize exactly what information is being transferred, to make certain that no required regulations are being violated. Otherwise, your organization could be on the receiving end of a significant financial penalty.

When it comes to using services like email marketing, business email, and text messaging, your company needs to be vigilant about conducting regular, in-depth reviews of exactly what information is being included and then to cross reference such content with the most current HIPAA regulations. Caveat Emptor! Official documentation from HIPAA does not accept ignorance as an explanation for errors of commission or omission. To the contrary, any breaches of unsecured PHI, whether or not intended, will result in a monetary settlement with the federal government, and possibly even an overhaul of related procedures that will cost your organization precious resources, both financial and administrative.

Addressable: while slightly more flexible in its meaning, addressable still requires a degree of examination and implementation of reasonably secure measures. The basic premise of addressable is that addressable does not mean optional! Unless an in-depth risk analysis concludes that implementation of given standards is not reasonable and appropriate specific to a given business, the relevant standards must be implemented. Your company is obligated to read and decipher each HIPAA security standard separately and to deal with each one in an independent fashion, in order to determine an approach that meets the needs of your organization. With an email marketing plan, for example, you need to review the content that will be disseminated electronically and if any potentially sensitive data is included or implied, such as healthcare-related content linked to individual email addresses, then privacy safeguards must be in place.

Rule # 1: Taking care of preventable problems applies not only to delivering quality health care, but also to following HIPAA guidelines. Exactly what kind of technology is permissible when sending email messages? The standards of the HIPAA Security Rule reflect a "technology neutral" stance. Rather than promote particular technologies, the rule takes into account the rapidly changing nature of information technology. It is important to note that technology neutral does not restrict vendor choice. The only requirement, therefore, is that all patient data be sufficiently protected. Four standards of the HIPAA Security Rule must be met:

Organizational Requirements refer to specific functions a covered entity must perform, including those related to business associate contracts, as well as to the development, documentation, and implementation of policies and procedures.

Administrative Requirements pertain to the training, professional development, and employee management with regard to PHI. Organizations are expected to implement security measures that reduce systemic risks and vulnerabilities to a reasonable and appropriate level to safeguard all electronic and physical information.

Physicl Safeguards protect workstations, computer servers, systems, and networks. Only authorized access to ePHI is allowed; access must be monitored through established policies and procedures that guard against violations. Additionally, security considerations apply to physical access to buildings, access to workstations, data backup, storage, and the destruction of obsolete data.

Technical Safeguards control access to ePHI and ensure the security of all data transmissions over an electronic network and to the storage of that data. These safeguards address issues involving the authentication of users, audit logs, data integrity, and data

CHAPTER 4

Risk Analysis & the Need for Encryption

Risk management is the key to HIPAA compliance. Each organization must diligently consider the risk of security and privacy violations to patient health information across the range of its workflow. Covered entities and their business associates must adopt certain measures to safeguard the security and integrity of ePHI from any reasonably anticipated threats or hazards. HIPAA encourages scalability and flexibility; each organization decides on those security measures and specific technologies appropriate to its best practices. Risk analysis methodologies will vary based on the size, complexity, and capabilities of an organization. It is important to keep in mind that risk analysis serves as the broad foundation of successful HIPAA compliance. After a thorough required yearly risk analyses and assessment of the organization's current security measures are undertaken, organizations may consider a cost analysis to determine the relative importance of potential gaps in security and privacy and the priorities for filling them.

Secure electronic communications start with 1) an evaluation of the practices, procedures, and policies that exist at the present time; 2) an enumeration of known and associated risks; 3) understanding precisely the requirements of the HIPAA security rule; and 4) developing a detailed risk mitigation strategy that outlines improvements and solutions to achieve HIPAA compliance.

Email encryption. What is it exactly? Encryption is a method that converts an original message of plain text into encoded text by means of an algorithm. Encrypting information greatly reduces the probability that anyone other than the intended recipient(s) would be able to read the emailed content.

Email communication certainly poses a multitude of security risks for any health care organization. Among the most common are unauthorized interception of sent messages, messages delivered to unauthorized recipients, either intentionally or in error, and stored messages that can be accessed by unauthorized persons. Encryption is essential!

Controls to address the risks inherent in the use of electronic communications are clearly spelled out in the "technical safeguards" section of the HIPAA security rule. Consider these three categories:

1 **Person or Entity Authentication** – (required) Procedures must be properly implemented to verify the identity of each person or system requesting access to ePHI. In other words, the identity must be confirmed within the information system being utilized. It also means, unequivocally, NO shared logins.

2 **Transmission Security** – (addressable) Data integrity controls and encryption have to be in place providing reasonable and appropriate safeguards.

3 **Business Associates** – If your organization outsources its email or messaging services to another company (the "business associate") and ePHI is included in any form, then your business associate must be HIPAA compliant, as well. Additionally, both parties must sign a special contract, the "business associate agreement." Your business associate is liable for actively safeguarding the ePHI of your organization that resides in or passes through their systems. Note that HIPAA's oversight of business associates' activity has become ever more stringent within the past decade.

Based on the technologies used to communicate ePHI, individual health care organizations determine how their email security standards will be implemented. All covered entities and business associates must implement security measures that guard against unauthorized access to ePHI that is transmitted over a network.

Addressable specifications of the technical kind include access control, automatic log off, encryption, and decryption. In the same category, covered entities must also assess organizational risks that relate to when transmission security is applicable. This includes integrity controls to ensure that improperly modified ePHI will not go undetected. While an addressable specification is extremely important for any ePHI publicly available on the Internet, it can be less so for ePHI that flowing between servers within an isolated, secure office infrastructure. Encryption of ePHI at rest – e.g. stored on a disk – is also an addressable specification, not a requirement, under HIPAA regulations. A heightened emphasis has been placed on at-rest encryption due to the risks and vulnerabilities not only of the Internet, but of portable storage devices. As decreed by the Department of Health and Human Services, covered entities and their respective business associates are obliged to exercise one of the following options with regard to such addressable specifications:

- Implement the specified standard.
- Develop and implement an acceptable alternative security measure to accomplish the intended purpose of the specified standard.
- Do not implement a specified standard, or alternative, if an organization objects that it is not reasonable and appropriate, even if it can still be met. But the choice must be documented. In this instance “reasonable and appropriate” relate to an organization’s technical environment and the security measures in place.

CHAPTER 5

Gmail and Google Apps?

Until 2013, Gmail and other Google applications were not completely HIPAA compliant, with the exception of a few cases where a covered entity had to sign a business associate agreement and pay a fee. Google has since made strides to ensure that its popular apps can safely fall under the auspices of HIPAA regulations and can be used by health care professionals.

The exact language comes straight from the horse's mouth:

HIPAA Compliance & Data Protection with Google Apps guide:

"Google Apps customers who are subject to HIPAA and wish to use Google Apps with PHI must sign a Business Associate Agreement (BAA) with Google. Per the Google BAA, PHI is allowed only in a subset of Google services. These Google covered services, which are "Included Functionality" under the HIPAA BAA, must be configured by IT administrators to help ensure that PHI is properly protected. In order to understand how the Included Functionality can be used in conjunction with PHI, we've divided the Google Apps Core Services ("Core Services") covered by your Google Apps Agreement into three categories. Google Apps administrators can limit which services are available to different groups of end users, depending on whether particular end users will use services with PHI.

1. HIPAA Included Functionality: All users can access this subset of Core Services for use with PHI under the Google Apps HIPAA BAA as long as the health care organization configures those services to be HIPAA compliant: Gmail, Google Drive (including Docs, Sheets, Slides, and Forms), Google Calendar, Google Sites, and Google Apps Vault.

2. Core Services where PHI is not permitted: There are certain remaining Core Services that may not be used in connection with PHI. Google Apps administrators can choose to turn on these remaining Core Services, which include Hangouts, Contacts, and Groups, for its users, but it is their responsibility to not store or manage PHI in those services. Please see "Separating user access within your domain" for further details on how to utilize organizational units.

3. Other Non-Core Services Offered by Google: PHI is not permitted in other NonCore Services offered by Google where Google has not made a separate HIPAA BAA available for use of such service. All other Non-Core Services not covered by your Google Apps Agreement, including, for example, (without limitation) YouTube, Google+, Blogger, and Picasa Web Albums must be disabled for Google Apps users who manage PHI within the Included Functionality. Only users who do not use Included Functionality to manage PHI may use those separate Non-Core Services offered by Google (under the separate terms applicable to these Google services). Please see "Separating user access within your domain" for further details on how to utilize organizational units."

With this unambiguous explanation, Google has moved forward to be quite specific on which core services are included in the HIPAA business associate agreement as well as how to separate user access to ensure that sensitive health information is not accidentally accessible via a Google App that is not included under HIPAA. As it is written in the guide: "To manage end user access to different sets of Google services, a Google Apps administrator can create organizational units to put end users who manage PHI and end users who do not into separate groups. Once these units are set up, the administrator can turn specific services on or off for groups of users."

In addition, Google Apps amended its business associate agreement in early 2015 to include Gmail, Google Calendar, Google Drive – including documents, sheets, slides and forms – Google Sites and Google Apps Vault to be included by their HIPAA business associate agreement. At the present time, however, these are still the only Google Apps that fully comply with the functional requirements of HIPAA compliance. No other Google services are HIPAA compliant and any use that exposes the data in a non-complaint way is not covered.

Entering into a business associate agreement with Google means that you implicitly agree to take "appropriate safeguards designed to prevent against unauthorized use or disclosure of PHI." That is the sum of what Google has to say

on the subject of business associate agreements and compliance requirements. Covered entities are left to fend for themselves and to know the right actions to take. Your business, not Google, will shoulder the added risk of potentially being in violation of HIPAA. Your business, not Google, will suffer any consequences.

Email encryption is NOT included with paid Google Apps accounts. Google does provide forced outbound Transport Layout Security (TLS) to email providers that support such encryption and Google does allow opportunistic TLS inbound and outbound, but your organization has no guarantee that communications are secure or that sent email messages will be HIPAA compliant. What you need is a mechanism that will, at a minimum, ensure that all messages are encrypted during transport, and allow recipients using non-HIPAA compliant email services to send secure messages back to you.

No such mechanism exists with a standard paid Google Apps account. Beware that if you sign up for Google Apps, request and sign their business associate agreement, and then proceed with sending emails, your organization very quickly will be in serious violation of HIPAA.

Google's business associate agreement is cursory and merely states that whatever is needed will be done within a reasonable time frame to ensure the privacy and security of any Google-held data. You assume responsibility for everything else. You especially do not want to send ePHI-laden email unless you have taken extra steps, at an extra cost, to ensure that the messages will be secure. And you definitely do not want to learn after the fact (because your organization will not discover this in advance) that Google provides no guidance about what should or should not be done to send email messages in a compliant manner.

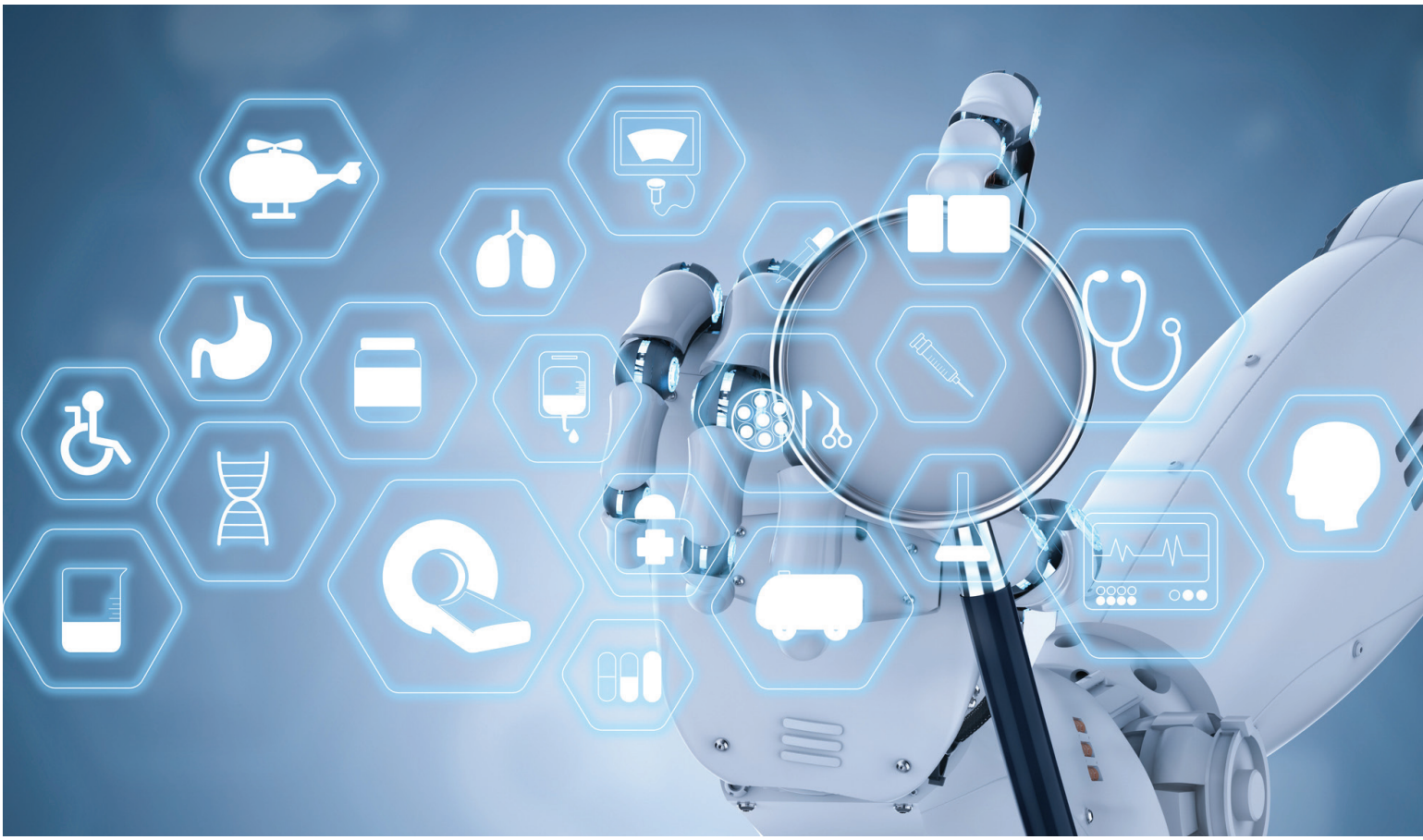
Yet Google does offer a message encryption solution called, and aptly named, Google Message Encryption. It provides a simple mechanism whereby email can be sent and retrieved from a secure web portal. But, the service will cost approximately $3 per user, per month. With Google's minimum requirement of 100 user licenses, you will soon be spending at least $300 monthly. Not an insignificant sum, for sure.

What alternatives are there to Google Apps and Google Message Encryption?
You can use a third-party HIPAA-compliant solution for your email encryption. Many of these are more feature-rich and more versatile than Google Message Encryption, providing the flexibility that you may need for your organization's business requirements. Most HIPAA-compliant third party email providers can service all of your email related needs (e.g. sending, receiving, filtering, archival, etc.) so that you do not even need Google Apps. Some can also hook directly into your Google user accounts and ensure that the email messages sent from them are secure; however, you will need to find a solution, purchase it, and configure it for use on top of your Google services. You also need to ensure that your chosen solution passes your risk analysis without taking their word for it. You need to know how it works so you know in what ways compliance is being met and in what ways it may not be. E.g. does the solution operate by relaying all messages from your Google Apps user accounts through the third party without authenticating the individual users to the third-party email system (i.e. without setting up usernames and passwords in Google for each user to connect to the third party system)? That could violate the HIPAA requirement for "person or entity authentication" preventing the third-party email system from truly knowing which Google Apps user sent each message and providing proper auditing.

CONCLUSION

The HIPAA requirements for electronic communication of patient health care may seem extensive and daunting. Be that as it may, you cannot afford to ignore the importance of being fully compliant with HIPAA. If patient ePHI is breached your business will likely suffer protracted legal wrangling with the Department of Health and Human Services and risk substantial financial penalties.

The risk of misuse of electronic patient data can never be totally eliminated, but it can be mitigated through careful, conscientious preparation. Due diligence is called for, to exclude those platforms and operations that do not have the capability for HIPAA compliance. The viability of your business depends on your attention to all electronic communications. It is ultimately your responsibility to be proactive about matters of security and privacy, and to minimize the risk of any HIPAA violations. You have the power to make sure that under your watch, electronic patient health information will be as safe as possible.



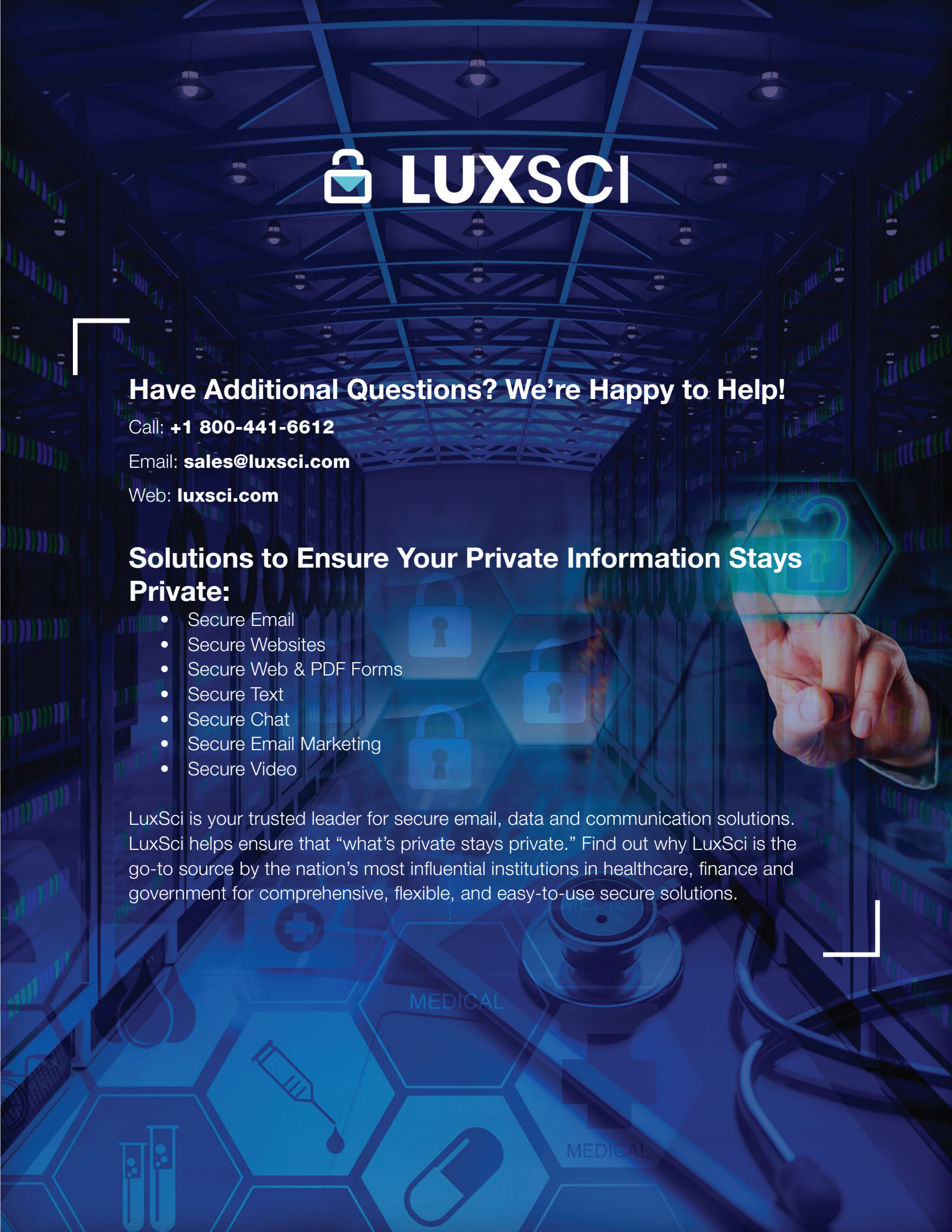
RESOURCES

http://www.hhs.gov/ocr/privacy/hipaa/faq/securityrule/2020.html

https://www.google.com/work/apps/terms/2015/1/hipaa_baa.html

http://linfordco.com/2013/09/required-vs-addressable-implementation-specifications-in-the-hipaa-security-rule/

https://static.googleusercontent.com/media/www.google.com/en/us/work/apps/terms/2015/1/hipaa_implementation_guide.pdf



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.