Healthcare Analytics and HIPAA:
Ways to Minimize Risk and Ensure Compliance

Joe Christopher
VP, Analytics - Blast Analytics

BLAST

Let's face it: our world continues to change in unforeseen and uncontrollable ways. Fortunately, healthcare organizations have shown an aptitude for transformation, whether addressing increased regulation, new service and cost models, emerging technology, and other areas designed to improve patient care. Today, healthcare organizations are faced with yet another critical challenge: patient data privacy.

With the Health Insurance Portability and Accountability Act (HIPAA) instituted in 1996, healthcare organizations must ensure that patient medical information is kept private. While securely managing patient data has been industry best practice for years, the rise in digital data and healthcare analytics creates added complexity -- and risk. Organizations that don't comply with HIPAA could face fines up to $50,000 per violation, as well as civil action lawsuits and criminal charges. Not to mention loss of patient trust.

HIPAA COMPLIANT

Yet this data and healthcare analytics provide organizations an immense opportunity to drive digital transformation and improve patient experience, particularly through marketing, on-site behavior, and personalization. Therefore, you must balance the requirement to protect consumer health information with the access and usage of patient data to drive greater results.

This white paper highlights the value and benefits of collecting and using digital data in healthcare organizations while providing an overview of HIPAA and associated risks of non-compliance. It also offers ways to assess your risk and ensure you have a roadmap in place to ensure compliance and patient data privacy for the foreseeable future. Lastly, it covers how proper data usage, including testing and personalization, can help optimize the patient experience.

Afterall, digital transformation and analytics are steering the future of healthcare. It's a delicate process maintaining compliance with government regulations such as HIPAA, given the volume of patient data sources. But with proper assessment, strategy, and guidance, you can become a healthcare analytics leader and EVOLVE your organization. to make important business decisions.

Healthcare Digital Analytics Usage and Benefits

In the rapidly changing and increasingly competitive healthcare industry, digital data analysis is essential for identifying insights and action to:

- Improve overall patient experience
- Ensure quality of care
- Reduce operational complexities
- Increase cost efficiencies
- Maximize revenue and profitability
- Maintain compliance
- Strengthen your position for long-term success

Healthcare organizations rely on patient data to make decisions that influence the above areas, however, your digital analytics platform can be a breach of security that leads to HIPAA non-compliance -- just one of many risks associated with healthcare data analysis.

Comprehending the benefits is the easy part. It's using the data in conjunction with analytics platforms that can be tricky when considered against patient privacy, and there's no room for error if your organization is going to comply with HIPAA.

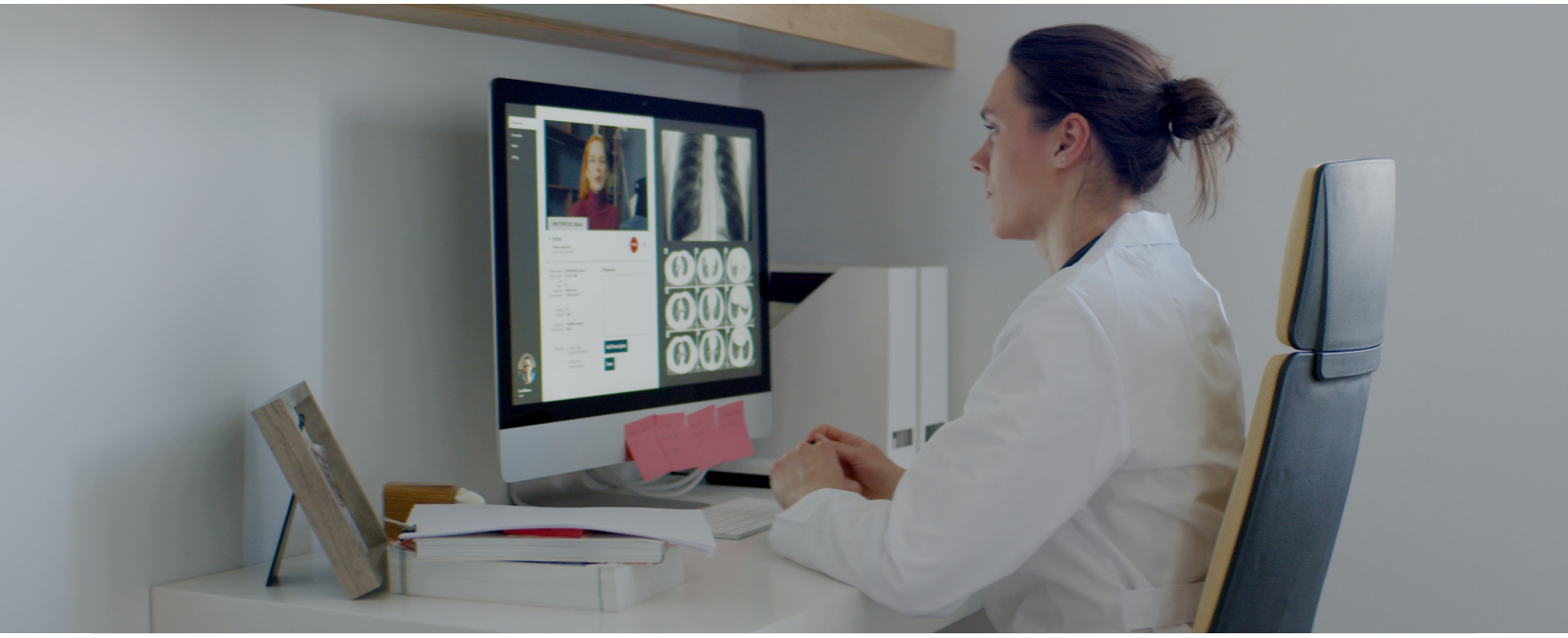
Assess Your Organization's Digital Analytics and Marketing Compliance Risk

To effectively assess your organization's compliance risks, you'll need to start with an audit. Your audit should:

- Examine the data you are sending to your digital analytics platform
- Determine what data is exposed in URLs and query string parameters
- Define the data send to the digital analytics platform
- Determine if identifiers are collected in the digital analytics platform (whether intentional or not)
- Identify which data is sent to marketing tags and determine how they leverage the collected data
- Determine how the collected marketing data in a third-party is being used to target users

After you've completed your audit, **you should prepare discussions with your privacy and legal team on the topic of HIPAA compliance**. It's not unusual for organizations to have to update these teams about the nature of the digital analytics tools they're using, as well as the nature of the data being collected and analyzed. In fact, it's important for these groups to review their chosen technologies and data management.

As your team identifies risks, you'll want to create strategies for minimizing or eliminating them. Is there a problem with your patient portal? Are there concerns about your organization's entire website? The audit is essential for helping you shape your approach to compliance.



Construct Your Compliance Roadmap

Compliance is invariably a process that involves many steps. Your organization's roadmap should prioritize the risks you've assessed and provide a structured, methodical approach to ensuring complete compliance.

As for navigating that roadmap, you'll need to remember that many platforms, such as Google Analytics 360 or Adobe Analytics, do NOT satisfy HIPAA requirements. To use these platforms safely, your organization will need to make some significant adjustments in order to avoid sending protected health information (PHI).

That said, these are best-in-class digital analytics platforms, and there are ways you can use these analytics solutions in order to gain the necessary insights while ensuring compliance.

Removing Protected Health Information

In order to mitigate your organization's data privacy risks, you can achieve compliant usage of your analytics tools by removing and no longer sending PHI. The U.S. Department of Health & Human Services provides two de-identification methods you can use:

1. Expert Determination Method
2. Safe Harbor Method

The Expert Determination Method features specific mandates that require documentation by a person with appropriate knowledge and experience who can authenticate that the data cannot identify an individual -- even when combined with reasonably available information.

The Safe Harbor Method addresses information removal from the data set. This method is ideal for organizations using Google Analytics 360 or Adobe Analytics. This de-identification method ensures that your data set is no longer regarded as protected health information.

Remember, you can't store PHI in Google Analytics 360 or Adobe Analytics. You must, in short, rely on the Safe Harbor Method to ensure that the data you're working with meets compliance measures.

Understand Protected Health Information

Although organizations should be aware of all 18 PHI identifiers outlined by HIPAA, the ones that are most commonly associated with digital analytics and marketing platforms include:

- Internet protocol addresses (IP addresses)
- Geographic data (specifically location data about the user that narrows at a more specific level than State)
- Email addresses
- Account numbers
- Device identifiers and serial numbers
- Web URLs (specifically those that contain information about a medical condition or other PHI data)

Removing Internet Protocol (IP) Address

To ensure compliance when using both Google Analytics 360 and Adobe Analytics, you may need to investigate sending data to these platforms server-to-server to reduce your risk. Here's why: The IP address is always transmitted when using a client-side deployment. While these platforms allow users to turn on IP Anonymization, there are still technical risks involved. You'll want to evaluate and discuss these risks with your legal and privacy teams.

Removing Geographic Data

In terms of geolocation, anything more specific than State level is regarded as PHI. If you prevent full IP address transmission to satisfy the de-identification requirements, then you may no longer have accurate geographic data. There are creative options here, such as performing geolocation in a compliant way (with a compliant provider), and then sending in just the State and Country values to your digital analytics tool.

Removing Account Numbers, Email Addresses, and Device Identifiers

To reduce your risks and ensure compliance, the advice is simple: don't perform data collection using these identifiers. By performing the privacy audit mentioned earlier, you'd have identified these risks and taken steps to mitigate them.

Removing Web URLs

Web URLs may be more tricky to manage. While your organization could choose not to collect Web URLs, that's in opposition to the way digital analytics tools are designed to work. Instead, make an assessment of whether a specific URL may be used to link a medical condition with a customer. For these URLs, you can include in a numeric page identifier rather than the complete URL. Keep in mind that Google Analytics 360 automatically collects Page Title; you'll have to address this issue, as well as maintain caution about querystring parameters, as these could prove to contain potential identifiers.

Mitigate Optimization and Personalization Risks

While navigating HIPAA compliance risks in association with analytics tools, you'll want to be mindful of the risks posed by optimization and personalization programs as well. Just as Google Analytics 360 and Adobe Analytics are not HIPAA-compliant, optimization tools like Google Optimize 360, Adobe Target, and Optimizely are also non-compliant with HIPAA. Consequently, if you're hoping to run an optimization or personalization program on your website/app, you must consider the risks and ensure that your program isn't compromising data privacy.

Google Analytics

Adobe

Your optimization tool will likely capture a number of data points by default. Like many digital analytics tools, optimization tools are typically loaded client-side. In other words, you install a third-party javascript snippet on your site that loads the optimization tool on each page of your site that a visitor visits. IP addresses are inherently transmitted during this client-side process, and other data points may be captured too. Unfortunately, even though most optimization tools offer IP Anonymization, anonymization only takes place right before processing, after the IP address has already been sent. So, technically, you're still liable for having sent the identifier. As with so many other risks, you'll need to discuss this one with your privacy and legal teams to determine the severity of this risk.

Choose the Best Approach to Compliance

There are two reliable approaches to achieve HIPAA compliance for optimization using your tool of choice. To select the best approach for your organization, consider the following:

- Types of tests/personalization campaigns you'll run
- How much technical support you have available
- Your budget for compliance-related updates

Your responses to these factors will help you choose between the two recommended approaches:

1. Using a HIPAA-compliant collection, storage, data-forwarding, and audience segmentation option, such as Tealium Private Cloud
2. Implementing your optimization tool server-side and ensuring you don't capture any PHI data (the Safe Harbor, de-identification process)

Both approaches will allow your testing program to comply with HIPAA, but it's important to choose an approach that fits best with your organization.

Personalization in the Healthcare Industry

Even if your organization is not actively pursuing a personalization strategy on your site now, it is well worth considering it for the future. Tech-savvy users are increasingly expecting personalized experiences across digital media, and that expectation will expand to their healthcare providers also. By implementing personalization on your sites, you can begin to explore personalized onsite experiences such as:

- Updating site copy and calls to action to encourage users to take desired steps. For example, creating accounts if they've never created one before, booking in-person or tele-appointments online if they're known to be patients, or re-ordering prescriptions when it's expected that their previous prescription is low.
- Tying onsite interactions to follow-up email marketing. For instance, if a user tries to schedule an appointment online, but doesn't complete the appointment setup, you can automatically send them an email recommending options to finalize their appointment.
- "Closing the loop" for users who've received email marketing campaigns. If users are in the audience that received an email campaign with a specific goal (i.e. review your latest test results online), then update the site to recommend they complete this action whether they visit the site via an email link or not.
- Rotating copy and content in primary communication spots on your site, such as the homepage banner, based on what content users have interacted with in the past. Currently, a lot of sites give the primary communication spots to COVID-19 updates, such as details on symptoms or how to get tested. If a user has already clicked on this content before, there's no need to promote it to them on every visit. You can personalize the user's experience by rotating the communications you show them. Next time they visit, highlight how to book a doctor's appointment by video rather than COVID-19 information, thereby ensuring the user is consistently being informed of all healthcare priorities and opportunities, rather than just the one.

There are many personalization options for healthcare providers, and the above are only a few of some common examples.

Maintain HIPAA Compliance with Testing and Personalization

To ensure compliance, you should review your tests and personalization campaigns just as you audit your usage of analytics tools. During your review process, be sure you understand how frequently you use data points such as geographic locations or triggered email campaigns based on a user's interactions with your site. You can see how easy HIPAA compliance may be compromised as organizations attempt to navigate the trickier aspects of privacy management and marketing prowess. Once your review is complete, you can take the necessary steps to mitigate your identified risks and ensure you're HIPAA-compliant.

Respecting the privacy of your patients and anonymous visitors to your websites or apps is essential to avoid non-compliance. By taking a proactive approach towards compliance, you'll build trust and avoid the costly risks associated with non-compliance. Privacy and security are part of a successful data governance program. It's extremely important to have a plan in place to continually audit your own compliance measures and identify risks. Most often, we see a combination of automated and manual audits that are scheduled at regular intervals.

As you approach compliance in the healthcare industry with your digital analytics and marketing solutions, please reach out to us if you need advice, have questions about analytics and compliance, or want our assistance.

About the Author: Joe Christopher

As Vice President, Analytics at Blast Analytics, Joe leads a team of talented, analytics consultants responsible for helping clients understand and take action on their vast amounts of data, to continuously improve and EVOLVE their organizations. With 20 years of experience in analytics and digital marketing, Joe is an expert in all major analytics platforms including Google Analytics and Adobe Analytics, as well as various tag management systems such as Tealium and Adobe Launch. He also consults on data visualization, data governance, and data quality strategies. Having extensive expertise in many areas, has enabled Joe to become a well known thought leader and speak at industry events such as Tealium's Digital Velocity series. Joe remains on the pulse of various information technology, programming languages, tools and services, keeping Blast and its clients on the leading edge.

Google Marketing Platform Sales Partner

Adobe Solution Partner
GOLD | SPECIALIZED
Adobe Analytics
Adobe Target

Optimizely

TEALIUM

tableau PARTNER

ObservePoint

Lytics

aws partner network

dynamic yield

salesforce

Tealium Certified Agency Partner

Optimizely CERTIFIED PARTNER

Microsoft

CONTENTSQUARE

Adobe

SNOWPLOW

Accredited Professional bing Ads

DoubleClick by Google

DOMO Professional Services CERTIFIED

DIGITAL ANALYTICS ASSOCIATION

BLAST

Roseville Office
950 Reserve Drive, Suite 150
Roseville, CA 95678

San Francisco Office
156 2nd Street
San Francisco, CA 94105

New York Office
54 West 40th Street
New York, NY 10018

Seattle Office
500 Yale Avenue North
Seattle, WA 98109

Los Angeles Office
7083 Hollywood Boulevard
Los Angeles, CA 90028

Chicago Office
220 North Green Street
Chicago, IL 60607

Dallas Office
1920 McKinney Avenue
Dallas, TX 75201

Washington, D.C. Office
1440 G Street NW
Washington, D.C. 20005

London Office
22 Upper Ground
London, UK SE1 9PD

www.blastanalytics.com | solutions@blastam.com | (888) 252-7866