HIPAA & GDPR eCommerce

Considerations and Recommendations

CLARITY

Overview

The UK and US legal requirements for medical websites generally fall into GDPR and HIPAA regulation guidelines (although GDPR isn't directly aimed at UK medical only). Overall, it makes sense to take a stance of complying with GDPR, HIPAA and other heightened security requirements. Clarity outlines a set of next steps and details associated with those below.

Clarity specializes in delivering custom results within a timely fashion – read more to find out how we can deliver for your organization.

Recommended Next Steps

Clarity recommends completing the following steps:

1. Enable hosting and auditing tools as shown in the detailed pricing and next steps section. The summary is that with a relatively simple minimum option the cost would vary between $400-$800/ month (depending on the options selected) to enable the hosting and auditing tools that will allow for a phase one that's reliable and enables core industry standards for compliance.

2. Enable compliance resource tool and review and follow guidelines with Azure, Clarity, and the compliance tool's support. There is a very reasonable offering from accountablehq.com for $400/month ($1,500/month if you'd like white-glove support and a dedicated compliance expert). This offering will provide, among other key outputs, a HIPAA Seal of Compliance (from Accountable), Compliance Dashboard, etc.

3. Set up recurring reviews (at minimum quarterly) to audit and review findings and complete any necessary updates (both within Client team and with Clarity, Microsoft, etc.).

4. As the business scales this offering, we recommend increasing the allocation of resources to 1-3 above and adding in more frequent reviews and execution on risk reduction measures.

Disclaimer

Clarity will work to enable the Client team to complete steps necessary for and maintain GDPR and HIPAA compliance. The overall requirements for GDPR and HIPAA are generally constant, however, the technical landscape is constantly changing. As a result, it's very likely that the Client team, Clarity, and/or other vendors involved in the delivery of the services, products and related support will need to complete ongoing maintenance, support and "patching" of the software and security as well as monitoring and review to enable GDPR and HIPAA capabilities. Although this document is intended to help provide resources to that end, it's not a comprehensive or complete document and should be considered as a helpful resource but not a definitive guide for each Client. Each Client project will be different, and we recommend ongoing and continual resources go into GDPR and HIPAA compliance to enable robust, long-term compliance.

Key Concepts

The overall concepts at play are generally related to the GDPR requirements and HIPAA requirements and overlaps between those. The primary tenets are:

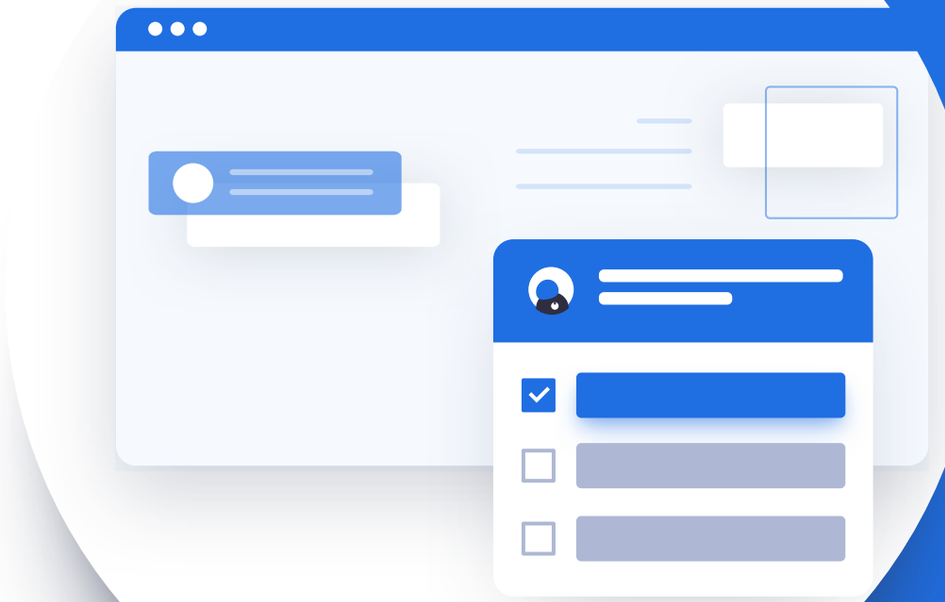
Industry Best Practices for Security

- Manage personal data with the appropriate security, including protection against unlawful or unauthorized processing, access, loss, destruction, or damage
- Ensure the confidentiality, integrity, and availability of all electronic protected health information
- Detect and safeguard against anticipated threats to the security of the information
- Protect against anticipated impermissible uses or disclosures
- Certify compliance by their workforce

Key Concepts

Privacy and Ability to Request Removal

- Fairly, lawfully, and transparently use personal data
- Use personal data for explicit, specific purposes
- Use personal data in an adequate, limited, and relevant way as necessary
- Maintain the accuracy of personal data and ensure up to date
- Assure that individuals' health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public's health and well-being
- Strike a balance that permits important uses of information, while protecting the privacy of people who seek care and healing



*Although there are nuances and much more extensive facets for each of these topics, the above provides an overall summary of the key concepts.

Service and Software Recommendations

Please note that Clarity will be happy to set up, configure and provide full ownership account information for the below recommended software and services. Clarity will also provide detailed training and support for the Client team to ensure if/when needed, the Client team can take over with managing and utilizing the software/services below.

1. Set up Microsoft Azure Hosting

- Utilize blueprints and enable GDPR, HIPAA oriented environment
- Set up Security Center and run audits to validate environment
- Enable ongoing support and review process with Client team

2. Set up service like AccountableHQ.com – see below for options:

- www.accountablehq.com/pricing
- www.compliancy-group.com
- www.capterra.com/hipaa-compliance-software

3. Set up service like Detectify.com – see below for options:

- https://detectify.com/product/deep-scan
- https://www.acunetix.com/product/standard/
- https://www.netsparker.com/product/
- https://www.clouddefense.ai/healthcare

Service and Software Recommendations

4. Set up service like Cloudflare.com – see below for options:

- www.cloudflare.com
- www.fastly.com
- www.g2.com/categories/content-delivery-network-cdn

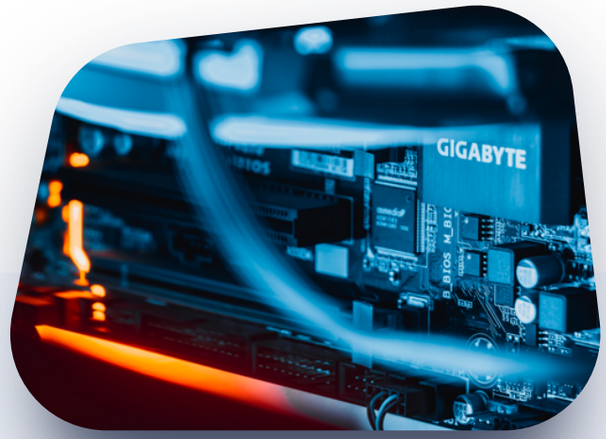
5. Set up service like Pingdom.com – see below for options:

- www.pingdom.com
- www.uptimerobot.com
- www.uptime.com
- www.g2.com/categories/website-monitoring

6. Run quarterly (or more often) QSA scans for PCI/DSS compliance and resolve any issues

- Azure Security Center
- www.qualys.com/apps/pci-compliance
- www.netwrix.com/PCI_Compliance.html

7. Set up BAA with Microsoft, Clarity, other service providers



Ongoing Organizational Recommendations

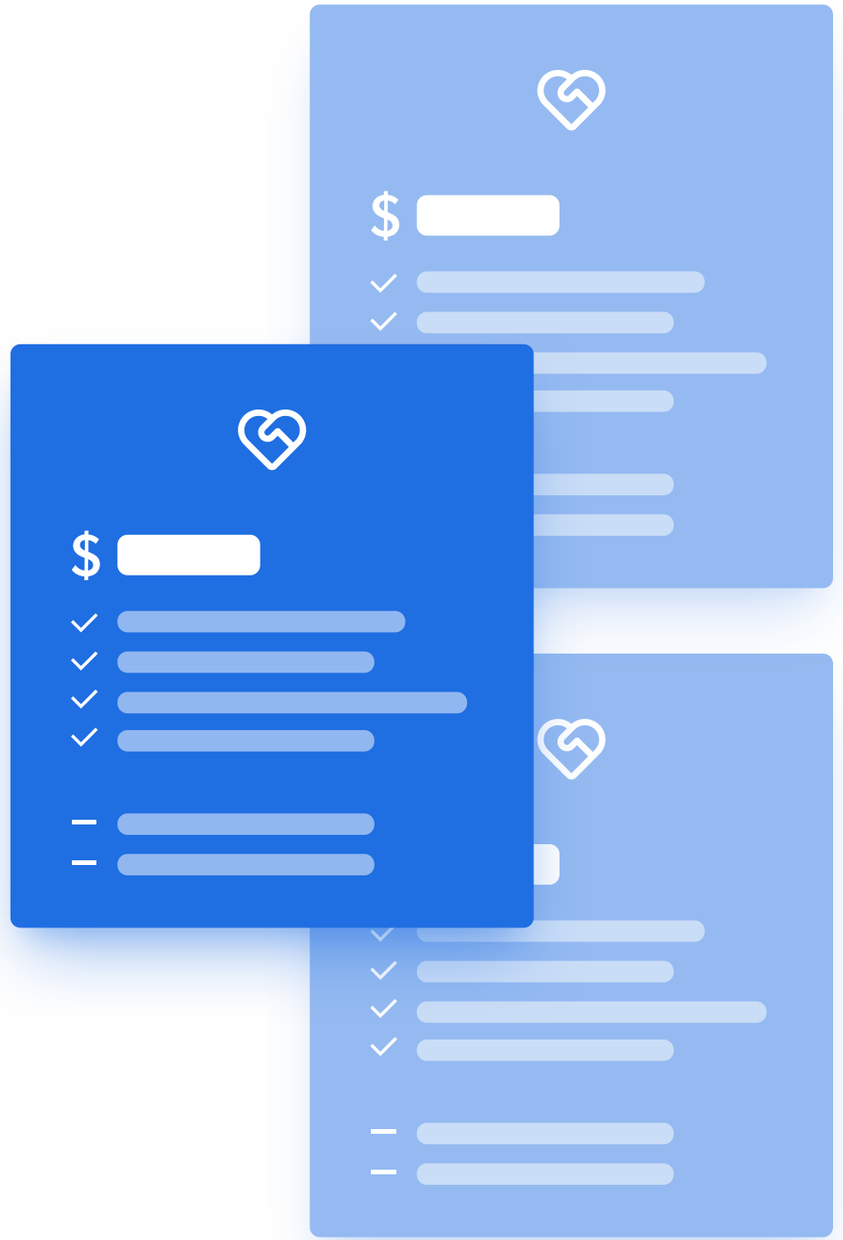
Clarity recommends setting up processes specific to GDPR and HIPAA compliance and working with services that will help enable these processes. In general, there will be internal and external processes that need to occur regularly. If possible, we recommend deputizing one or more individuals within the organization to complete training and become compliance officers or similar, internally. This can be a relatively small-time commitment – in other words a role that gets added to their existing responsibilities.

A simple way to enable this process adjustment is to leverage a service that helps guide and manage the process overall. One example of these offerings is www.AccountableHQ.com. The main outcome that will need to occur is regular auditing of the key responsibilities, auditing of the responsible parties, and ongoing validation of the organization's adherence to the GDPR and HIPAA compliance. There are many options for setting this up, but generally this is something that requires ongoing auditing and review. Leveraging a third-party resource makes the process much simpler overall and can help reduce the risk associated with otherwise manually completing the audits and ongoing research internally.

Detailed Pricing and Next Steps

Although the pricing will vary based on usage and scale, generally the Azure configuration will range from $200-$800/ month based on the selections the Client team makes for services and robustness of the infrastructure.

The Clarity team recommends a detailed review with the Client team to establish specific pricing and selections for each of the above categories with regards to CDN, security pen-testing, site uptime auditing, PCI-DSS compliance validation, etc. If the Client team elects to use the recommended services shown above, the monthly cost for the additional services will range from roughly $200-$400/month in fees. Although these aren't required services, they can each help to enhance compliance and overall robustness of the overall solution the Client team is able to bring to bear within the market.



Detailed Pricing and Next Steps

Azure | Blueprints and Setup

- Apply GDPR
  - https://azure.microsoft.com/en-us/blog/protecting-privacy-in-microsoft-azure-gdpr-azure-policy-updates/
  - https://docs.microsoft.com/en-us/compliance/regulatory/gdpr-dsr-vsts?view=o365-worldwide
- Apply UK Official and UK NHS Blueprints
  - https://docs.microsoft.com/en-us/azure/governance/blueprints/samples/ukofficial/
- Apply HIPAA HITRUST 9.2
  - https://smb.blob.core.windows.net/smbproduction/Content/Microsoft_Cloud_Healthcare_HIPAA_Security_Privacy.pdf
  - https://azure.microsoft.com/mediahandler/files/resourcefiles/a-practical-guide-to-designing-secure-health-solutions-using-microsoft-azure/A_Practical_Guide_to_Designing_Secure_Health_Solutions_using_Microsoft_Azure.pdf
  - https://azure.microsoft.com/en-us/blog/microsoft-releases-automation-for-hipaa-hitrust-compliance/
  - https://docs.microsoft.com/en-us/azure/governance/blueprints/samples/hipaa-hitrust-9-2
- Include full implementation of Azure Security Center and Azure Policy
  - https://azure.microsoft.com/en-us/services/azure-policy/#security

Recommended Responsibility Matrix

Generally speaking, the Microsoft Azure and Clarity offering falls into a PaaS solution model, such that the Client team will be responsible for Identity & Access management, Client & end-point protection, and Data classification & accountability. Microsoft Azure will be responsible for the Physical Security, Host infrastructure, Network controls and Application-level controls. Clarity will generally be responsible for the Application-level controls and Identity and Access management functionality.

Shared Responsibilities

The widely understood cloud service models as defined in the NIST Definition of Cloud Computing Special Publication 800-145 are infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS). The service model that is chosen by customers also dictates the responsibilities of managing their cloud environment. The diagram on the next page shows the split in responsibilities by key areas and is critical for all customers to understand, but especially those in regulated industries as they assess and mitigate risks.

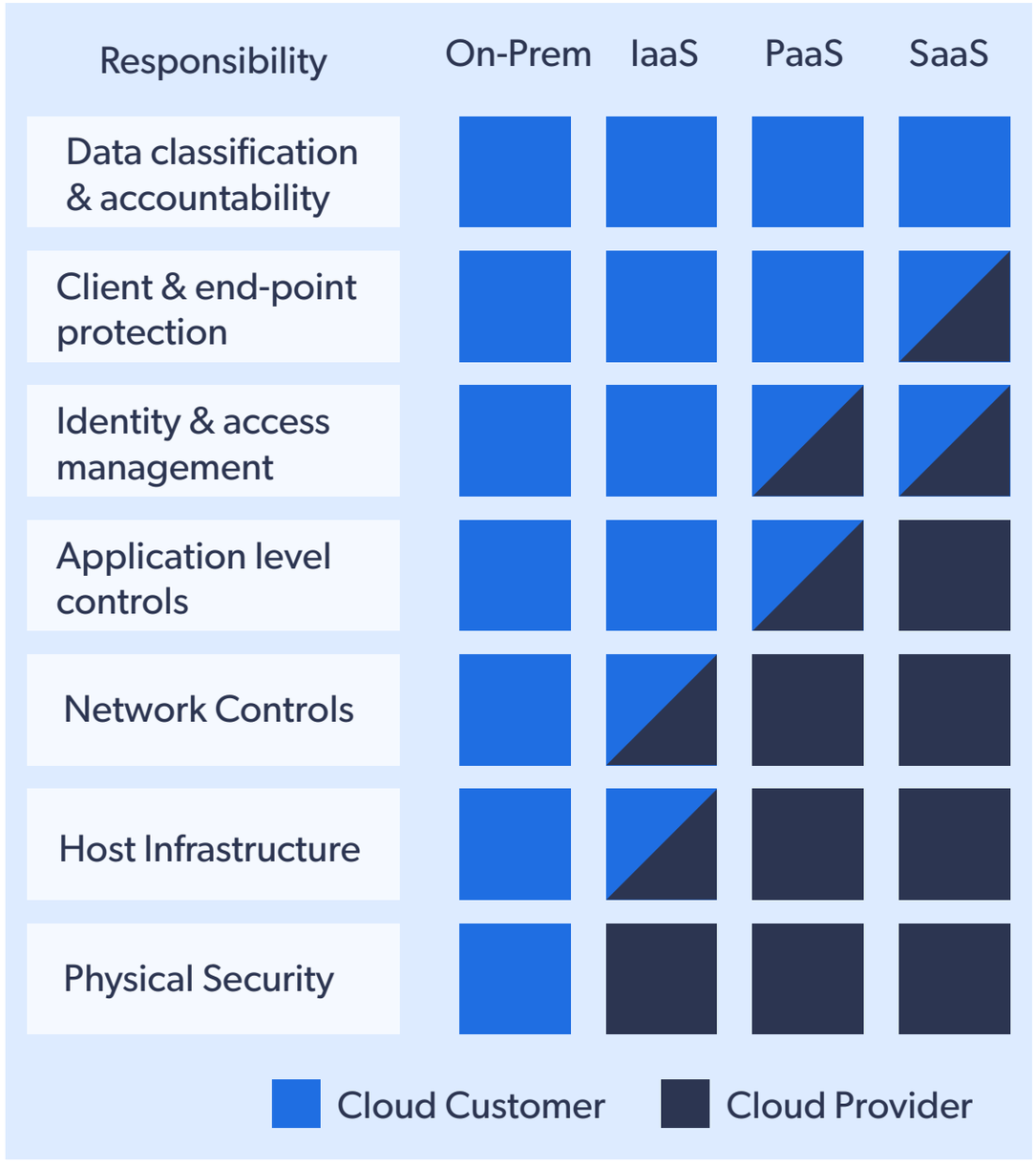
- The customer is completely responsible for all aspects of operations when solutions are deployed on-premises.

Recommended Responsibility Matrix

- With IaaS, the lower levels of the stack, physical hosts or servers, and host security are managed by the platform vendor. The customer is still responsible for securing and managing the operating system, network configuration, applications, identity, clients, and data. For the developer, an obvious benefit with IaaS is that it reduces the developer requirement in configuring physical computers.

- With PaaS, everything from network connectivity through the runtime or identity service may be provided and managed by the platform vendor. PaaS offerings further reduce the developer burden by additional supporting the platform runtime and related appliation services. With PaaS, the developer can almost immediately begin creating the business logic for an application.

- With SaaS, a vendor provides the application and abstracts customers from all of the underlying components. Nonetheless, the customer continues to be responsible to ensure that data is classified correctly and that user devices are secured and protected when connected to the service.



Clarity Can Help

Healthcare and Medical Web Development

With nearly 1,000 websites under our belt, Clarity proves to be an industry leader in web technology. We help organizations with everything web, including our scalable eCommerce platform, back-office integrations (EMR, ERP, and CRM), our own medical scheduling application and custom website designs. Our team has over 300 years of combined design and development experience delivering websites from small businesses to Fortune 500 enterprises, like Disney and the USO.

Although Clarity has designed and built websites for virtually every vertical, we have dozens of clients in the healthcare and medical industries. As we develop for these companies, we work with expert project managers and consultants who specialize in the healthcare and medical fields.

Through these relationships and successful projects, Clarity partners with our own medical consultants and project managers, bringing you not only the industry's best web and development technologies, but consultants who can help ensure what we build is exactly what you need to drive your business.

> **Clarity walked with us step-by-step through a minefield of global regulatory compliance as we built a multi portal website in 6 languages with regionalized product information, multimedia content, and customized content management interfaces. We came in on-time and under budget.**
>
> Dana Kolflat, Global Project Lead, LDR Spine

Website Development & Our Clients

In addition to knowing how to design and develop your website, Clarity has experience developing platform-independent and mobile-friendly custom applications for our healthcare and medical device clients:

- Find a Physician / Office / Clinic locators
- Payment / subscription processing for plans and insurance claims
- Patient education and product launch portals and press media kits
- Secure sales and scheduling portals
- CRM and EMR application integrations
- HIPAA compliant websites, patient forms and appointment scheduling
- Product / device digital flipbooks for doctor's and surgeon's offices
- Medical education and sales program management applications

Get in Touch with Clarity

If you are a business, ready to move forward with your project,
please give us a call or visit our website.

+1 (800) 928 - 8160

clarity-ventures.com

Tyler Wiener

Executive Account Manager

tyler.wiener@claritymis.com

Philip Ganoe

Executive Account Manager

philip.ganoe@claritymis.com

CLARITY