onelogin

SOLUTION BRIEF

HIPAA Compliance Solution

www.onelogin.com | **twitter.com/onelogin**

OneLogin, Inc. | 150 Spear Street, Suite 1400, San Francisco, CA 94015

855.426.7227

OneLogin does not store any electronic protected health information (ePHI), so it does not significantly alter your current or planned HIPAA controls. However, OneLogin can augment your HIPAA compliance efforts by providing your IT system administrators with additional functionality that can be leveraged to support the alignment of your IT control environment with HIPAA requirements. In addition, it is important to note that companies subject to HIPAA, should include OneLogin as part of their risk assessment performed in response to HIPAA Security reference §164.308(a)(1)(ii)(A).

Risk Area: Access Management [HIPAA Security references §164.308(a)(1)(ii)(B), §164.308(a)(3)(i), §164.308(a)(3)(ii)(A), §164.308(a)(3)(ii)(C), §164.308(a)(4)(ii)(B), §164.308(a)(4)(ii)(C), §164.312(a)(1)]

Granting and removing access to applications can be done either through the OneLogin portal, or if you set up directory integration, through your existing LDAP directory. By establishing or mapping your existing roles and groups to OneLogin, you can quickly grant, modify, or remove access based on role based privileges that are as granular as you need to make them. With real time LDAP to OneLogin updates, changes you make in your local directory system are immediately pushed to OneLogin, thus removing the need for you to have to update several access lists or having to wait for a batch program to process in a timely and complete manner.

Example Scenario: Access Management

Your company has summer interns that help book patient appointments using an online scheduling system, so you create a "Summer Intern 2014" role that gives them access to the scheduling system, email, and several other office productivity apps. Once the internship is over, you remove their access by simply deleting the entire role in the OneLogin Portal or deactivating the LDAP group that is mapped to that role in your local directory system.

Risk Area: Segregation of Duties [HIPAA Security references §164.308(a)(3)(i)]

Roles and groups in OneLogin also help you plan your segregation of duties strategy by allowing you to map out pre-defined access levels and document any authorized exceptions based on your own organizational structure and resource pool.

Example Scenario: Segregation of Duties

A senior accountant needs access to do a final check at month end of all bills that were issued and all bills that were collected. He is given a provisional "End of Month" role for him to review the bills in the coding and billing system on top of his standard "Accounting" role. In addition, OneLogin creates a login audit trail to correlate the end of month process with his access granting and subsequent logging into the coding and billing system.

Risk Area: Authentication [HIPAA Security references §164.308(a)(5)(ii)(D), §164.312(a)(2)(iii), §164.312(d)]

Not all applications support the same, or robust enough, password requirements. This requires you to keep track of the various password requirements and in extreme cases, having to explain to your auditors how you compensate for weak password requirements. OneLogin allows you to centrally manage one or more password policies in addition to providing you with a multi-factor authentication option. This allows you to create a more robust authentication scheme for remote users or for users of high risk applications, including timing out sessions as needed.

Example Scenario: Authentication

Your quarterly OneLogin roles report review helps you identify a user that no longer needs access to an application that stores ePHI. After updating their access, you review the logs to validate that they did not access the application during the relevant timeframe.

Audit Evidence: When undergoing HIPAA assessments, auditors will request a lot of documentation, including several access control lists and evidence that access was granted appropriately for those in scope. Instead of chasing down several access lists or trying to evidence that the list of users with access to ePHI is complete and accurate, if you are using OneLogin as your central point of access management and authentication, you will greatly reduce the HIPAA audit level of effort and documentation needs.

About the Author

Alvaro Hoyos is the Director, Risk & Compliance for OneLogin, Inc. He has over 8 years of compliance experience working for PwC and Grant Thornton, two of the largest global public accounting firms. During that time he provided local and national leadership in the areas of SSAE 16, SOC 2, FedRAMP, FISMA, and SOX 404. He also has extensive experience working with Cloud Service Providers in the Bay Area and has been in the IT field for over 16 years.