To Whom It May Concern:

sookasa

This document serves as a formal letter of attestation for the recent HIPAA security review undertaken by your company. Praetorian analyzed the safeguards of the Sookasa application between the dates of February 4, 2015 and April 10, 2015. Based on the evidence collected from the HIPAA security review, Praetorian has concluded that the Sookasa application has implemented an adequate set of security controls to satisfy HIPAA technical safeguard requirements. Consequently, a user that uses Dropbox in conjunction with Sookasa and follows HIPAA procedures can sustain HIPAA compliance.

Praetorian believes that the statements made in this document provide an accurate assessment of Sookasa's current security as it relates to HIPAA technical safeguard requirements. This professional opinion does not include an evaluation of other technical security controls that, while considered industry best practice, are not explicitly defined in the HIPAA technical safeguard requirements. As the Sookasa application's code base changes, and new features and functions are added, the Sookasa application's security posture will change. Such changes may affect the validity of this letter. Therefore, the conclusion reached from our analysis only represents a "snap-shot" in time. Praetorian would like to thank Sookasa for this opportunity to help the organization evaluate its current security posture.

Sincerely,

Nathan Sportsman
Chief Executive Officer, Praetorian
nathan.sportsman@praetorian.com

Table 1, HIPAA Technical Safeguard Requirements

HIPAA Technical Safeguards		
164.312(a)(1)	**Access Controls**	**Technical policies and procedures for electronic information systems that maintain EPHI to allow access only to those persons or software programs that have been granted access rights as specified in Sec. 164.308(a)(4).**
164.312(a)(2)(i)	Unique User Identification. Assignment of a unique name and/or number for identifying and tracking user identity	Requirement satisfied. Each user is assigned a unique username (email address) and a password. This credential set is used for identifying and tracking user identity
164.312(a)(2)(ii)	Emergency Access Procedure. Established (and implemented as needed) procedures for obtaining necessary EPHI during and emergency	Requirement satisfied. An administration "dashboard" provides administrators a way for obtaining necessary EPHI in the event of an emergency
164.312(a)(2)(iii)	Automatic Logoff Procedures that terminate an electronic session after a predetermined time of inactivity	Requirement satisfied. The application has a configurable session timeout with a default value of 30 minutes.
164.312(a)(2)(iv)	Encryption and Decryption. A mechanism to encrypt and decrypt EPHI	Requirement satisfied. Sookasa allows encryption and decryption of electronic protected health information via its PC, Mac and iOS clients as well as via a web browser interface
164.312(b)	**Audit Controls**	**Hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use EPHI**
Not applicable	This standard has no implementation specifications.	Requirement satisfied. Sookasa provides complete audit trails on all operations associated with encrypted files with a simple reporting tool

164.312(c)(1)	**Integrity**	**Implement policies and procedures to protect EPHI from improper alteration or destruction.**
164.312(c)(2)	Electronic mechanisms to corroborate that EPHI has not been altered or destroyed in an unauthorized manner	Requirement satisfied. HMAC signatures ensures integrity of EPHI stored at rest
164.312(d)	Person or Entity Authentication procedures to verify that a person or entity seeking access EPHI is the one claimed	Requirement satisfied. Authentication and authorization controls properly enforce access to EPHI
164.312(e)(1)	**Transmission Security**	**Technical security measures to guard against unauthorized access to EPHI that is being transmitted over an electronic communications network**
164.312(e)(2)(i)	Security measures to ensure that electronically transmitted EPHI is not improperly modified without detection until disposed of	Requirement satisfied. SSL/TLS ensures the integrity of EPHI passed in transit.
164.312(e)(2)(ii)	A mechanism to encrypt EPHI whenever deemed appropriate	Requirement satisfied. The Sookasa application encrypts information prior to its upload to Dropbox