Hushmail HIPAA and security checklist

01 Security management policies and procedures

- [ ] 1.1 Hushmail has policies and procedures that meet all applicable HIPAA requirements.
- [ ] 1.2 Hushmail has policies and procedures that clearly define how to prevent, detect, contain, and correct security matters.
- [ ] 1.3 Hushmail has policies and procedures in place to ensure that electronic Protected Health Information (ePHI) only resides on machines identified for that purpose.
- [ ] 1.4 Hushmail regularly inventories all hardware and software that reside on all organization machines.
- [ ] 1.5 Hushmail has a formal process in place to address system misuse and abuse, as well as fraudulent activity by employees within Hushmail.
- [ ] 1.6 Hushmail regularly reviews records to ensure that hardware and systems have not been tampered with and that the records contained within these hardware and systems have not been compromised.
- [ ] 1.7 Hushmail has assigned an employee the responsibility of maintaining policies and procedures.
- [ ] 1.8 Hushmail reviews applicable documentation periodically to ensure that it's up to date with respect to changes to standards, as well as changes within Hushmail.
- [ ] 1.9 Hushmail documents changes to its policies and procedures and retains all documentation for a minimum of six years.
- [ ] 1.10 Hushmail policies and procedures are accessible by employees on an as needed basis.

02 Security responsibility

- ☑ 2.1 Hushmail maintains complete job descriptions that accurately reflect assigned security duties and responsibilities.
- ☑ 2.2 Hushmail has an employee dedicated to the security of ePHI.

03 Workforce security

- ☑ 3.1 Hushmail has policies and procedures in place so that non-authorized employees cannot gain access to ePHI.
- ☑ 3.2 Only Hushmail employees who need access to ePHI as part of their role are given access, and Hushmail regularly reviews and documents the employees who have access to ePHI.
- ☑ 3.3 Background checks are completed for new employees.
- ☑ 3.4 Hushmail has procedures in place to revoke ePHI access privileges from employees who are terminated or no longer need such access.

04 Information access management

- ☑ 4.1 Hushmail has policies and procedures in place that clearly define how access is granted to employees.
- ☑ 4.2 Employees within Hushmail have unique logins such that each login is connected to only one employee.
- ☑ 4.3 Hushmail maintains documented job descriptions that accurately reflect assigned duties and responsibilities and enforce segregation of duties.
- ☑ 4.4 Hushmail has policies and procedures in place, including usernames and passwords, to secure access controls.
- ☑ 4.5 Authorized employees can gain access to systems in the event of an emergency.
- ☑ 4.6 Hushmail has systems and procedures in place that send alerts if access authorizations have been inappropriately altered.
- ☑ 4.7 Hushmail encrypts the disks that contain ePHI ensuring that, if they were stolen, the data would be unreadable.

05 Security awareness and training

- 5.1 Hushmail regularly trains employees on the rules and procedures for working with ePHI.
- 5.2 Hushmail sends out periodic reminders to employees regarding security procedures.
- 5.3 Hushmail employees must annually read and attest to their having read Hushmail's policies and procedures.
- 5.4 Hushmail requires computers to have anti-virus or other protection software installed.
- 5.5 Hushmail has systems in place to report when excessive system login failures occur.
- 5.6 Hushmail systems lock accounts when excessive failed login attempts have occurred.
- 5.7 Hushmail requires strong passwords.
- 5.8 Hushmail employees are required to regularly change their passwords.
- 5.9 Hushmail has two-factor authentication in place for employee system access.

06 Security incidents

- 6.1 Hushmail documents and tracks known security incidents.
- 6.2 Hushmail informs its customers of security incidents when they directly affect their ePHI.

07 Contingency plan

- 7.1 Hushmail backs up its ePHI data in a manner that is not easily readable onto servers and encrypted disks.
- 7.2 Hushmail has procedures in place to restore ePHI should any data be lost.
- 7.3 Hushmail periodically tests emergency operation modes to ensure they work.

08 Business associate and other agreements

- 8.1 Hushmail allows certain outside business associates access to its ePHI.
- 8.2 Hushmail creates written agreements with these parties to ensure they abide by the policies and procedures implemented within Hushmail and detail how they must handle ePHI.
- 8.3 Hushmail periodically reviews the practices of these external parties to ensure they are appropriately handling ePHI.
- 8.4 These parties know, and the agreements require, that they must report security incidents back to Hushmail should they occur.
- 8.5 Hushmail is able to terminate these agreements if they violate the terms of the contract.

09 Facility access

- 9.1 Machines that house ePHI are stored in a facility that has physical access controls, such as electronic key locks.
- 9.2 These facilities can be accessed by authorized employees during an emergency.
- 9.3 Hushmail employees and/or partners are validated for authorization prior to entering these facilities.

10 Workstation use and security

- 10.1 Hushmail is aware of all machines that have access to ePHI.
- 10.2 Hushmail has security measures in place to ensure non-authorized workstations cannot gain access to ePHI.
- 10.3 Hushmail ensures that all machines that have access to ePHI are not accessible by unauthorized individuals.

11 Device and media controls

- 11.1 Hushmail properly disposes of hardware that contains ePHI.
- 11.2 Hushmail ensures that all ePHI has been removed from a device prior to reusing that device.
- 11.3 Hushmail keeps records of the devices that once contained ePHI but are repurposed for other uses or disposed of.
- 11.4 Hushmail ensures backup of a device prior to deleting ePHI from it.

12 Audit controls

- 12.1 The systems that contain ePHI log all audit events, including who performed those events.