Information Security Policy

V1.0

ALL CONTENTS ARE CONFIDENTIAL

Purpose: To provide clients, consultants and contractors with a general overview of WebMD Ignite information security program. This document is not meant to constitute or convey all of WebMD Ignite policies, standards or procedures which are detailed in formal documentation located elsewhere.

1. Definitions

1.1. Capitalized terms not otherwise defined in this, WebMD Ignite's Information Security Policy, have the respective definitions assigned to them in other parts of the Agreement.

1.2. "DMZ" is defined as a computer host or small network inserted as a "neutral zone" between a company's private network and the outside public network.

1.3. "Minimum Necessary" is defined as limiting the amount of information disclosed to the minimum necessary to achieve the specified goal (consistent with CFR 164.514(d)(1)).

1.4. "Protected Information" or "PI" includes all information protected under various legislative and state and federal regulatory requirements including, but not limited to, Gramm-Leach-Bliley ("GLB") for financial information, Health Insurance Portability and Accountability Act of 1996 ("HIPAA-AS") for Protected Health Information ("PHI"), the Privacy Act, agency requirements for federal and state health programs (Medicare, Medicaid, Federal Employee Program, etc.), as well as any applicable state restrictions on sensitive health data. It also applies to information transmitted or maintained electronically, orally, on paper or other media.

1.5. "Constructive Custody" is defined as when the customer PHI remains on the customer's network and WebMD Ignite only has controlled access to the customer PHI, through a presentation layer.

1.6. "Actual Custody" is defined as when the customer PHI physically resides on WebMD Ignite's network or passes through WebMD Ignite's network to the customer.

2. Compliance with Security Requirements

2.1. WebMD Ignite has implemented the security measures set forth herein and maintains documentation confirming such implementation. Documentation is available upon request of a client and available for audit onsite at select WebMD Ignite offices or online via a WebMD Ignite defined video conference tool.

2.2. WebMD Ignite meets the requirements and responsibilities concerning the processing of PHI as defined in relevant HIPAA Business Associate Agreements which shall take precedence over this document in cases of conflict concerning PHI.

3. Safeguarding Procedures

3.1. WebMD Ignite has established and maintains physical, technical, administrative, environmental, safety and facility procedures, data security procedures and other safeguards against the destruction, loss, theft, unauthorized access or alteration of PHI in the actual or constructive custody, possession or control of WebMD Ignite or WebMD Ignite Personnel. Respective procedures and safeguards:

3.1.1. are no less rigorous than the good industry practices followed by tier-one service providers of outsourced services;

3.1.2. are no less rigorous than those maintained by WebMD Ignite for its own information of a similar nature or for other customers of WebMD Ignite with respect to information of a similar nature; and

3.1.3. meets the requirements of any and all applicable Data Privacy Laws including state governed law.

3.2. With respect to PHI in WebMD Ignite's actual custody, possession or control, WebMD Ignite makes reasonable commercial efforts to maintain backup security or backup copies of PHI Data.

3.3. With respect to PHI in WebMD Ignite's actual custody, possession or control, WebMD Ignite regularly, and no less than annually, evaluates, tests and monitors the effectiveness of its information security program; promptly adjusting and/or updating it as reasonably warranted by the results of such evaluation, testing and monitoring.

3.4. Without limiting the generality of Section 3.1.1 above, the information protection plan provides for:

3.4.1. industry standard security systems, computers and technologies, including firewalls, encryption and/or reasonably equivalent security controls;

3.4.2. physical security procedures, including regular monitoring of all work areas, secure business facilities, data centers paper files, servers, back-up systems and computing equipment, including all mobile devices and other equipment with information storage capability;

3.4.3. appropriate background checks on WebMD Ignite Personnel and other personnel;

3.4.4. restriction of use and copying of PHI on a minimum necessary basis and only at authorized locations;

3.4.5. regular monitoring of the transport and storage of PHI;

3.4.6. regular monitoring of password procedures;

3.4.7. regular monitoring of WebMD Ignite Personnel and other employees providing Services or working on systems and programs;

3.4.8. access reviews;

3.4.9. network, device application, database and platform security.

3.5. With respect to PHI in WebMD Ignite's actual custody, possession or control:

3.5.1. encryption of PHI placed on any electronic notebook, portable hard drive or removable electronic media with information storage capability, such as compact discs, USB drives, flash drives, tapes:

3.5.2. encryption of PHI when in transit over insecure networks and, when appropriate, at rest;

3.5.3. PHI must not be processed, loaded, used or otherwise placed in test, development or non-production environments unless necessary to fulfill contractual service obligations.

3.5.4. intentionally deleted;

3.5.5. access to PHI outside of normal application activity must be logged and monitored; and

3.5.6. WebMD Ignite Personnel with access to PHI are provided appropriate information security and privacy training to ensure their compliance with WebMD Ignite's obligations and restrictions under this Agreement, with Data Privacy Laws and with WebMD Ignite's information security program.

4. Data Access

4.1. Right to access. See section 27, Security Audit Rights.

4.2. WebMD Ignite grants access to PHI to authorized WebMD Ignite Personnel only as permitted by contract and corresponding Business Associate Agreement; and

4.3. WebMD Ignite regularly reviews access to PHI to ensure access has only been granted to authorized Personnel.

5. Certification

5.1. WebMD Ignite maintains information security certification(s) from firm(s) that specialize in enterprise information security assessment and certification. The certification program may include either (1) a properly scoped SOC 2 Type 2 review that includes assessment of the entire IT infrastructure that supports the Services provided by WebMD Ignite and related security policies and practices or (2) a HITRUST certification on products that accept, transmit, and store PHI data dependent upon the product/offering.

6. PHI Sharing or Transfer

6.1. Clients must provide WebMD Ignite with written authorization at least thirty (30) days prior to requiring that WebMD Ignite share or transfer PHI to clients' affiliates, subcontractors or other third parties (including but not limited to CD, DVD, USB drive or network-based information transfers) on their behalf;

6.2. For all network-based PHI transfers between end users andWebMD Ignite involving PHI, WebMD Ignite uses secure transmission methods (such as private circuits, frame relay connections, virtually private encrypted connections, or encrypted information transfer protocols), as described herein:

6.3. WebMD Ignite transfers network-based PHI between WebMD Ignite and any other third party via an appropriately secure method such as:

- **6.3.1.** via a private network between WebMD Ignite and the other third party (such as a private circuit, MPLS connection or frame relay connection);
- **6.3.2.** if sent over the open Internet, via a wholly encrypted communication tunnel (such as Local Area Network (LAN) to LAN Virtual Private Network (VPN)); or
- **6.3.3.** if sent using File Transfer Protocol (FTP), via an encrypted information transfer protocol;
- **6.3.4.** WebMD Ignite utilizes secure protocols to move or transfer PHI over internal networks owned/operated by Vendor, subcontractors or other third parties; and
- **6.3.5.** Vendor, subcontractor, or other third party must use encrypted Email when transmitting restricted confidential and proprietary data, including PHI, by email.

7. Backup Requirements for PHI in WebMD Ignite's Actual Possession, Custody or Control

7.1. WebMD Ignite maintains backup copies of PHI in accordance with a documented backup plan developed by Product Engineering teams and approved by WebMD IgniteManagement.

7.2. Where WebMD Ignite uses offsite backup facilities as part of its backup plan, all sensitive (PHI) data is encrypted on the backup media and the encryption key is stored separately from the media at all times.

7.3. All backup media is stored in a secured area accessible only by authorized individuals.

7.4. Where WebMD Ignite maintains its own backup media as part of its backup plan, WebMD Ignite also maintains a log of all parties entering/exiting the area where the backup media is kept. Additionally, a process and procedure for conducting regular log reviews for persons entering the area has been implemented.

7.5. Where WebMD Ignite outsources media storage services as part of its backup plan, WebMD Ignite requires applicable security measures to maintain appropriate access controls in order to ensure the confidentiality, integrity and availability of PHI data are maintained by our third-party vendors.

8. Disposal and Lingering PHI in WebMD Ignite's Actual Possession, Custody or Control

8.1. WebMD Ignite, without unreasonable delay, removes electronic PHI from temporary locations controlled by WebMD Ignite (such as, but not limited to laptops, workstations, web servers, FTP servers, database servers or test environments) after the intended business purpose has passed.

8.2. WebMD Ignite removes all electronic PHI, prior to disposal of storage media it owns, utilizing industry-accepted secure methods such as those described by the National Institute of Standards and Technology to clear, purge or destroy the storage media.

8.3. WebMD Ignite documents the disposal of any hardware or media (such as, but not limited to tape drives, thumb drives, diskettes, compact discs (CD's), digital video discs (DVDs), laptop drives, workstation drives or server drives) storing PHI.

8.4. Documentation includes equipment description, serial numbers, dates of disposal, reason for disposal, method of disposal and individuals performing the disposal.

9. Data Protection

9.1. PHI in actual custody of WebMD Ignite is secured as required by HIPAA regulation. This includes physical and technical security ensuring that PHI cannot be removed from premises, and encryption using a minimum of Advanced Encryption Standard (AES) 128 when physical security is not sufficient.

10. Training

10.1. WebMD Ignite Personnel (employees, independent contractors, subcontractors, consultants or other third parties) that handle PHI must complete a security/privacy awareness training course prior to accessing any restricted confidential and proprietary data, including PHI and periodically (at least once every twelve (12) months) thereafter complete update and refresher security/privacy training;

10.2. Training includes administrator and end-user responsibilities as applicable, as well as applicable administrative, technical, and physical information security controls; and

10.3. Training is documented, including the names and confirmation of those individuals who received the training.

11. Wireless (802.11)

11.1. WebMD Ignite uses wireless network communication (802.11) in its environment, and PHI is accessible wirelessly by authorized WebMD IgniteHealthcare Personnel.

11.2. WebMD Ignite supports and utilizes appropriate wireless security mechanisms for the intended purpose of the device but in all cases, at least those minimum mechanisms below unless otherwise mutually agreed to:

- 11.2.1. strong encryption (minimum WPA2);
- 11.2.2. the wireless LAN must be segmented from the wired network utilizing a firewall if/whenever appropriate; and

11.3. Any built-in wireless technologies in end point devices is set for manual connection unless the network is protected as described in clause (11.2) above.

12. Logging and Monitoring

12.1. In regard to systems accessing, storing or processing PHI, WebMD Ignite has logging and log monitoring policies and procedures and has an ongoing log analysis process consistent with the relevant HIPAA regulations and requirements.

13. Intrusion Prevention and Detection

13.1. WebMD Ignite has implemented a network-based intrusion detection system (IDS)/intrusion protection system (IPS) solution for network segments containing systems accessing, storing or processing PHI.

14. Authentication and Passwords

14.1. WebMD Ignite has developed, documented and adheres to an identity verification process.

14.2. WebMD Ignite adheres, where technically feasible, to the following account password policy for all systems (network devices and hosts) using guidance provided by the NIST 800-63B publication:

- 14.2.1. Passphrase methodology;
- 14.2.2. Requires minimum of 14 characters;
- 14.2.3. No repeated spaces;
- 14.2.4. No password reset requirements.
- 14.2.5. invokes a thirty (30) minute account lock-out after an excessive number of consecutive failed attempts (5); and
- 14.2.6. requires an appropriately secure mechanism (e.g. an administrator or automated challenge response system) to verify the user's identity prior to early reinstatement of the account.
- 14.2.7. Where not technically feasible the following may be used:
  - 14.2.7.1. password complexity;
  - 14.2.7.2. periodic password changes;
  - 14.2.7.3. a password history be configured to prevent passwords from being reused;
  - 14.2.7.4. require an account lock-out after an excessive number of consecutive failed attempts; and

14.2.7.5. require an appropriately secure mechanism (e.g. an administrator or automated challenge response system) to verify the user's identity prior to reinstating the account.

14.3. Usernames or passwords are not to be shared or transferred among WebMD Ignite Personnel without authorization.

15. Infrastructure Architecture

15.1. WebMD Ignite does not store any PHI on a device located on a DMZ segment. The data must be stored on an internal segment and accessed by the application layer of the application providing such access. Virtual environments can be used, but must maintain the separation described above (i.e., cannot have DMZ and Internal virtual hosts on the same physical device).

16. Patch Management

16.1. WebMD Ignite has developed, documented, and adheres to a reasonable patch management process consistent with relevant industry best practices for all relevant aspects of WebMD Ignite's environment.

16.2. WebMD Ignite applies applicable critical security patches or other risk mitigation measures as determined by WebMD Ignite's classification of criticality in the appropriate and most timely manner to both protect the security of the environment and maintain continuous operations of the systems; and

16.3. WebMD Ignite applies applicable non-critical security patches or other risk mitigation measures on at least a quarterly basis.

17. Vulnerability Scanning and Penetration Testing

17.1. WebMD Ignite has developed, documented, and adheres to vulnerability scanning policies and procedures consistent with industry best practice for systems that handle PHI data.

17.2. WebMD Ignite conducts vulnerability scans at least annually.

17.2.1. All Internet-facing applications that access, store or process PHI are scanned prior to production implementation to verify that all applicable Open Web Application Security Project (OWASP) Top 10 vulnerabilities have been prevented.

17.2.2. Vulnerabilities identified during scanning or penetration testing are fixed and/or other risk mitigation measures are put in place without unreasonable delay.

18. Web Hosting

18.1. In the event that WebMD Ignite provides services that include the hosting of content online, the specific requirements for hosting arrangements in which users (including, but not limited to, customers, employees, etc.) access WebMD Ignite's website from an external website, must be defined and mutually agreed to in the relevant service-specific purchase or service agreement.

19. Software

19.1. All WebMD Ignite Personnel are prohibited from installing any software not pre-approved by WebMD Ignite's software management policy on any hardware that may access, store or process PHI; and

19.2. WebMD Ignite restricts the implementation of keystroke monitoring software/hardware on systems processing and/or storing PHI.

20. Device and Host Configuration Controls

20.1. WebMD Ignite hardens operating systems, utilizing the least amount of services required.

20.2. WebMD Ignite has implemented Virus Protection as follows:

20.2.1. All at risk hardware must have current antivirus software protection installed or an acceptable alternative when 'conventional' 3rd party antivirus software is not supported by the device manufacturer; and

20.2.2. All at risk hardware used must have up-to-date virus definitions, updated at frequent, regular intervals, preferably once per day;

20.2.3. WebMD Ignite has implemented automatic lockout for electronic sessions on any hardware (i.e., laptops, workstations, mobile devices, servers, etc.) that access, store, or process PHI. The screen and/or console locks after 15 minutes of inactivity and requires the user to re-authenticate.

21. Removable Media

21.1. WebMD Ignite limits the use of removable media (such as, but not limited to, universal serial bus (USB) drives, CDs, Laptops, cameras) by WebMD Ignite or WebMD Ignite Personnel to only media owned or supplied by WebMD Ignite;

21.2. WebMD IgnitePersonnel do not connect personally owned removable media to any hardware that is used to access or process PHI;

21.3. WebMD Ignite encrypts, using a WebMD Ignite corporate solution, any and all removable media used for storage of PHI. The encryption software utilizes at least AES-128 encryption; and

21.4. Removable media may not be used for storage or transportation of PHI data, except for sanctioned and secure transportation to AWS.

22. Remote Access

22.1. Remote Access to WebMD Ignite's Internal Network.

22.1.1. For all remote access to WebMD Ignite's internal network for any reason, traffic with the remote device must be encrypted and the remote user must utilize strong authentication.

22.1.2. WebMD Ignite has a policy and/or technical controls covering acceptable use of remote access from a public location (e.g., airports, coffee shops, etc.) prohibiting access to PHI via unsecured networks.

22.1.3. WebMD Ignite has a policy and/or technical controls covering acceptable use of remote access from a public location (e.g., airports, coffee shops, etc.) and

prohibiting any inadvertent exposure of PHI to unauthorized persons in public places.[1]

22.1.4. WebMD Ignite has policies and technical controls restricting remote access connectivity using mobile devices or personal devices.

23. Physical Security Plan

23.1. WebMD Ignite limits physical access to work areas and to systems that may store PHI to only those WebMD IgnitePersonnel that have a business need for such access.

23.2. WebMD Ignite documents all physical security controls and supplies such documentation to clients for review upon the client's request and reasonable suspicion of a contract or security breach.

23.2.1. Such reviews must take place in person at the WebMD Ignite offices or online via a WebMD Ignite defined video conference tool.

23.3. WebMD Ignite has implemented the following physical security controls in locations where PHI is stored and/or accessed:

23.3.1. Electronically controlled access, restricting access to only those with a business need;

23.3.2. a clean desk policy for staff; and

23.3.3. Cameras, with recording capability, at all entrances to locations with storage of sensitive data.

24. Business Continuity

24.1. WebMD Ignite has a business continuity plan in place to ensure that the goods and/or Services contracted for will be delivered in accordance with mutually agreeable schedules. These plans also address the performance failure of WebMD Ignite's subcontractors.

25. Disaster Recovery

25.1. WebMD Ignite has a disaster recovery plan in place, to ensure its ability to restore any loss of data. These plans address the performance failure of WebMD Ignite's subcontractors.

25.2. The disaster recovery plan is regularly tested, at least annually, the results of such testing driving the identification and implementation of updates and adjustments to the plan.

26. Documentation Sharing

26.1. Policy documentation is maintained by WebMD Ignite and made available for client review upon request. All reviews must take place in person at one of the WebMD Ignite offices or online via WebMD Ignite defined video conference tool.

26.1.1. WebMD Ignite does not provide policy, standard, procedure or plan documentation to external parties directly.

26.1.2. Clients may schedule reviews to take place at select WebMD Ignite offices when desired.

27. Security Audit Rights

27.1. Upon reasonable suspicion of a security breach or non-compliance that could affect client confidential data, clients have the right to perform an audit through a mutually approved third party at WebMD Ignite's site including but not limited to an on-site visit and inspection of physical security measures, data security measures, status of third party certifications, compliance with HIPAA requirements and the condition of WebMD Ignite's facility.

For additional questions or to schedule a review of WebMD Ignite's security or privacy policies, standards, procedures contact either the CISO or Privacy Officer.

Title	Name	Email
Chief Information Security Officer	Marjo Mercado	marjo.mercado@internetbrands.com
Privacy Officer	Katherine Wich Sugden	katherine.wichsugden@internetbrands.com