Maimonides Medical Center

CODE: INFO TECH 015 (Recoded Reissued)
DATE: September 09, 2022
ORIGINALLY ISSUED: August 22, 2019 AS MIS PC015

SUBJECT: Cloud Services Providers

I. POLICY:

The purpose of this policy is to ensure that all Cloud Services (defined below) that are purchased by, or installed in, Maimonides Medical Center Enterprise Network (MMCEN or "Maimonides Network") adhere to industry best practices that are outlined in this document. The technical requirements outlined in this policy are for the sole purpose of maintaining the confidentiality, integrity and availability of the data in the Medical Center's possession. The devices covered by this policy include, but are not limited to, servers, desktop computers, laptops, printers, wireless access points, hand-held devices, switches, firewalls and routers. This policy also includes any device or system that is placed on segregated network within MMCEN but, interfaces with other systems on the MMCEN. This specifically refers to biomedical equipment which interfaces with the MMCEN.

II. RESPONSIBILITY

A. The Chief Technology Officer and the Security Officer will have overall responsibility for policy adherence.

B. All Maimonides employees who have the authority to evaluate, recommend, purchase or approve a system must adhere to this policy.

III. DEFINITIONS

A. "Cloud Services" means providing online access to shared computing resources including, without limitation, cloud-based email, document storage, Software-as-a-Service, Infrastructure-as-a-Service, Platform-as-a-Service, etc. Cloud Services specifically include, but are not limited to, the following: GMail, Google Docs, Google Drive, Hotmail, Box.com, Dropbox, Office 365, Yahoo Mail, or any similar service. If it is uncertain as to whether a particular service is cloud-based, please contact the MIS Department.

B. "Cloud Services Provider" or "CSP" means all vendors providing services to Maimonides that either (1) directly provide Cloud Services to Maimonides or (2) use one or more subcontractors (a "Cloud Services Subcontractor") to provide Cloud Services to Maimonides.

C. "Protected health information" or "PHI" consists of any patient (or employee) information, including very basic information such as name or age, that (1) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and (2) either identifies the individual, or could reasonably be used to identify the individual. Protected health information may be in any form, including spoken, written, or electronic form. Examples of protected health information include, but are not limited to, medical records, medical data on information systems, and applications for health or disability benefits. "EPHI" (Electronic Protected Health Information) is PHI transmitted by or maintained in electronic media.

D. "Personal Identifying Information" or "PII" consists of any information concerning a person which (1) can be used to identify such person because of name, number, personal mark, or other identifier and (2) also consists of one or more of the following data elements: Social Security number, Driver's License number or Non-Driver identification card number; mother's maiden name; surname prior to marriage; home address; telephone number; email address; internet ID name; or account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to a person's financial account.

IV. PROCEDURES:

A. General Guidelines for Cloud Services

- MMC Users are not permitted to use any Cloud Services to store, share, archive, manipulate or otherwise exchange Maimonides EPHI or PII Data unless done in accordance with this policy.
- All CSP's are required to complete Maimonides Information Security Assessment for Cloud Solutions. It is the responsibility of Maimonides sponsor to ensure the Information Security Assessment is completed before a solution is selected.
- Use of all Cloud Services must be specifically authorized by the HIPAA Privacy Officer, HIPAA Security Officer, CIO, CTO or their designee. The HIPAA Privacy Officer, HIPAA Security Officer, CIO, CTO or their designee will certify that security, privacy and all other IT management requirements will be adequately addressed by the CSP.
- If a CSP requires MMC Users to agree to terms of service (e.g., through an End User License Agreement), such agreement(s) must be reviewed and approved by the HIPAA Privacy Officer, HIPAA Security Officer, CIO, CTO or their designee.
- A fully executed Business Associate Agreement with the CSP must be reviewed and approved by Maimonides General Counsel and HIPAA Privacy Officer. (See policy HIPAA-002, "Business Associates.")

- It is the decision of the HIPAA Privacy Officer, HIPAA Security Officer, CIO, CTO or their designee to define which Maimonides workflows and data may be moved to a Cloud Services environment. There are no exceptions.

B. Architecture and Software Isolation Disclosure
All CSPs must:

- will share the architecture and underlying technologies it uses, including the implications that the technical controls involved have on the security and privacy of the system, over the full system lifecycle and across all system components.
- will define and whiteboard their software isolation strategy with Maimonides Information Technology Team upon request and define which logical isolation techniques it employs in any multi-tenant software architecture.
- Provide timeline for advancing its infrastructure from a Public Cloud proprietary architecture (i.e. AWS) to a Containerized Applications configuration and Kubernetes

C. Identity and Access Management

All CSPs must:

- ensure that adequate safeguards are in place for identity and access management that are used to secure authentication, authorization, and other identity and access management functions.
- to the extent practicable, integrate with Maimonides' Directory Services for authentication and authorization. If integration with Maimonides Directory Services (including, but not limited to, Federated Services, LDAP or Azure AD) is unavailable at the time of implementation, the CSP must provide a timeline for integration.
- Describe your strategy for multi-factor authentication and SAML Identity Provider integration.
- provide Maimonides with all system access logs, activity logs and event logs within ten (10) business days of request.
- provide Maimonides with annual compliance audit reports performed by an independent agency upon request.

D. Data Protection

All CSPs must:

- identify the data protection control standard it uses (e.g., HITRUST, NIST, etc.) for its data management solution and define its ability to control access to data;
- Identify the encryption protocols and standards used to
    - Encrypt data at rest and allow us to hold the encryption keys.
    - Secure data in transit.
    - Protections for data in use.

- use site to site VPN IPSEC connection for system data exchanges, interface or otherwise, to eliminate man-in-the-middle attacks. Maimonides will not be forced to open any internal server or other system component to the internet outside of the VPN site-to-site tunnel
- detail the environment's use of IP access control restrictions including, but not limited to
    - IP Whitelisting
    - Geolocation IP Fencing
    - Impossible Travel Alerting
    - Intrusion Detection Systems (IDSs)
    - Intrusion Prevention Systems (IPSs)

- with respect to Maimonides data, not deviate from the mutually agreed upon data protection and access controls (e.g., the CSP will not permit any direct access to Maimonides data via the internet).
- Ensure that Maimonides data including EPHI, (Electronic Protected Health Information), PII (Personal Identifiable Information) or any de-identified data is not shared with, viewed, accessed by or sold to another entity.
- Controls must be in place to ensure that Maimonides data resides in data centers within the continental United States.
- Permit vulnerability and penetration testing by Maimonides Medical Center or an authorized subcontractor and remediate all security vulnerabilities affecting the cloud environment at no additional cost to Maimonides. Such vulnerabilities include, but are not limited to, deprecated security protocols, unsupported operating systems and zero-day exploits.
- upon request, share with Maimonides the patching and maintenance schedule for all components of the cloud environment.
- demonstrate that the use of its services complies with all pertinent laws and regulations governing the handling of EPHI, PII, corporate financial data or any other Maimonides data.

E. Availability

All CSPs must:

- provide your uptime availability SLAs including any exceptions to those guarantees.

- for any Cloud Service Subcontractors, it uses, identify the contract provisions and procedures regarding data availability, data backup and recovery, and disaster recovery such that Maimonides IT personnel may ensure that such provisions and procedures meet Maimonides's continuity and contingency planning requirements.
- ensure that during an intermediate or prolonged disruption or a serious disaster its critical operations (and those of its Cloud Services Subcontractors) can be immediately resumed, and that all operations can be reinstituted in a timely and organized manner.

- Require downtime workflow or procedures to provide business continuity in the event of an Internet outage or other disruption.

F. Incident Response and Disclosure

All CSPs must:

- ensure that any Cloud Services Subcontractors it uses will clearly identify the provisions and procedures for incident response in the arrangement between such Cloud Services Subcontractor and the CSP.
- in the event of a Breach or Security Incident (each as defined at 45 C.F.R. Part 164) or any other unauthorized acquisition of Maimonides EPHI or PII, ensure that Maimonides can respond to incidents in a coordinated and transparent fashion with the CSP and, if applicable, the Cloud Services Subcontractor.
- notify Maimonides IT team as soon as practicable (but no later than 10 business days from the discovery date) regarding a Breach or Security Incident (each as defined at 45 C.F.R. Part 164) or any other unauthorized acquisition of Maimonides EPHI or PII .

IV. CONTROLS:

A. It is the responsibility of the Management Information Systems Department to ensure that the controls necessary for enforcing the policy's goals are in place.

B. HIPAA Privacy Officer, HIPAA Security Officer, CIO, CTO or their designee have overall responsibility for policy adherence.

C. The Human Resources Department shall assist in implementing this policy and with disciplinary actions relating to violations.

Kenneth Gibbs
President & CEO

REFERENCE(S):

45 C.F.R. Parts 160 & 164; N.Y. General Business Law §899-aa; U.S. Department of Health and Human Services Office for Civil Rights (OCR), "Guidance on HIPAA and Cloud Computing," October 6, 2016 (available at https://www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html)
Maimonides Information Security Assessment for Cloud Solutions

INDEX:	Cloud Computing, Privacy, HIPAA
DEPARTMENT RESPONSIBLE::	Information Tech
ATTACHMENT(S):	None