Manifest MedEx
Participant Policies and Procedures
July 2022

TABLE OF CONTENTS

GLOSSARY OF DEFINED TERMS

This Section defines terms that are used in MX's Policies and Procedural Requirements (the "**Policies**"). Any terms used in these Policies that are not defined herein shall have the definition set forth in the Agreement. Unless a specific MX Policy indicates otherwise, the following terms have the meaning set forth below:

1. ***Applicant*** means any Healthcare Provider or Health Plan that wishes to become a Participant of MX.

2. ***Application*** means software approved or certified by MX for the purpose of accessing Patient Data through the MX System.

3. ***Application for Participation*** means an Applicant's application to become a Participant of MX.

4. ***Authorization*** shall have the meaning and include the requirements set forth at 45 CFR § 164.508 of the HIPAA Regulations and include any similar but additional requirements under applicable Law.

5. ***Authorized User*** means an individual designated, in accordance with the procedures set forth in the Participation Agreement, by an Administrator to access and/or use the Services on behalf of a Participant, and who is permitted under applicable Law to use the Services.

6. ***Authorized User Entities*** means all facilities, practice sites, and affiliated organizations of an Applicant on behalf of which the Applicant proposes to obtain and/or facilitate access to Healthcare Data through the MX System and/or Services.

7. ***Board of Directors*** is the Board of Directors of MX.

8. ***Breach of Privacy or Security*** means the access, use, receipt, or disclosure of Patient Data (including electronic PHI) that is not in compliance with Law.

9. ***Business Associate*** has the meaning ascribed to this term in 45 C.F.R. § 160.103.

10. ***Business Associate Agreement ("BAA")*** is the business associate agreement that is executed by a Participant and MX and attached to the Agreement.

11. ***CMIA*** means the California Confidentiality of Medical Information Act, California Civil Code Section 56 *et. seq.*

12. ***Covered Entity*** has the meaning ascribed to this term in 45 C.F.R. § 160.103.

13. ***De-Identified Data*** means data that satisfies the requirements of 45 C.F.R. § 164.514(b).

14. ***Exchange Framework*** means a national or regional health information network (HIN), health information exchange (HIE), or health information exchange framework.

15. ***Excluded Health Information*** means information under federal or California law the disclosure of which is prohibited or restricted as set forth in a list provided by MX, which list can change over time depending on the changes in applicable law and/or the changes in technology. The current list of Excluded Health Information is: (i) psychotherapy notes; (ii) records of federally-assisted alcohol and drug abuse treatment facilities and programs, the confidentiality of which is

protected under federal regulations at 42 C.F.R. Part 2, as well as information from state sponsored substance abuse treatment programs protected under California law; (iii) outpatient psychotherapy records and mental health information (medical information related to mental health services) protected under California law; (iv) personal information collected by hereditarydisorders programs conducted under the auspices of the California Department of Public Health; (v) records of persons receiving state funded services for developmental disabilities; and (vi) HIVtest results.

16. ***Failed Access Attempt*** means an instance in which an Authorized User attempting to access the MX System is denied access due to use of an inaccurate log-in, password, or other security token.

17. ***Healthcare Operations*** means Healthcare Operations as defined in 45 C.F.R. § 164.501, including conducting quality assessment and improvement activities, population-based activities relating to improving health or reducing Healthcare costs, and case management and care coordination; reviewing the competence or qualifications of Healthcare professionals, evaluating provider and health plan performance, training Healthcare and non-Healthcare professionals, accreditation, certification, licensing, or credentialing activities.

18. ***Health Plan*** means Participant that either: (a) meets the definition of health plan in HIPAA; or (b) provides core health plan administrative services (at a minimum: medical claims processing services and provider network management services) to a health plan that meets the HIPAA definition.

19. ***Healthcare Data*** means Patient Data and/or De-Identified Data collected, created, maintained, or disclosed by MX.

20. ***Healthcare Provider*** means Participant that either: (a) meets the definition of provider in HIPAA; or (b) is a medical group (e.g., independent practice association) providing core administrative services to a provider that meets the HIPAA definition.

21. ***HIPAA*** means the Health Insurance Portability and Accountability Act of 1996, as amended by HITECH, and the regulations promulgated thereunder at 45 C.F.R. Parts 160 and 164.

22. ***HIPAA Privacy Rule*** means the federal regulations at 45 C.F.R Part 160 and Subparts A and E of Part 164.

23. ***HIPAA Security Rule*** means the federal regulations at 45 C.F.R Part 160 and Subpart C of Part 164.

24. ***HITECH*** means the Health Information Technology for Economic and Clinical Health Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (commonly known as "ARRA"), Pub. L. No. 111-5 (February 17, 2009).

25. ***Including***, include and words of similar import will be deemed to be followed by the words "without limitation."

26. ***Independent Practice Association*** means an association of independent physicians or small groups of physicians that is owned by physicians and formed for the purpose of contracting with one or more managed health care organizations.

27. ***Law*** means any federal, state or local law, statute, ordinance, rule, legally binding administrative interpretation, regulation, order, judgment, or decree that is applicable to a Party or to another

Person identified in this Agreement.

28. ***Limited Data Set*** means PHI from which "facial" identifiers have been removed. Specifically, as it relates to the individual or his or her relatives, employers or household members, identifiers must be removed except for (1) dates such as admission, discharge, service, data of birth, or date of death; (2) city, state, five digit or more zip code; and ages in years, months or days or hours.

29. ***Longitudinal Patient Record or LPR*** means the longitudinal patient records maintained by MX.

30. ***Marketing*** has the meaning ascribed to this term under the HIPAA Privacy Rule as amended by Section 13406 of HITECH.

31. ***MX Administrator*** means the MX Privacy Officer and/or his/her designees, who shall be responsible for issuing credentials for the System for MX Personnel and for other responsibilities delegated by MX.

32. ***MX Personnel*** means MX and MX's employees, subcontractors and subcontractors' employees providing any part of the System or the Services.

33. ***MX Privacy Officer*** means the individual appointed by MX to oversee the privacy policies and practices of MX.

34. ***MX Security Officer*** means the individual appointed by MX to oversee the security policies and practices of MX.

35. ***MX Vendor*** means a vendor with which MX has contracted with to provide technology in connection with providing Services.

36. ***Offshore*** means outside of the United States of America and its territories.

37. ***Opt-Out*** means the decision made by a Patient/Member to not allow access to Patient Data relating to him or her through MX, made and effectuated through a Patient/Member's execution and submission of Opt-Out form(s).

38. ***Participant*** means the Person that has entered into a Participation Agreement with MX.

39. ***Participant Administrator*** means the representative(s) of Participant designated in accordance with these Policies who is responsible for designating Authorized Users of Participant and for other responsibilities delegated by Participant. Each Participant Administrator is automatically designated an Authorized User of the Services.

40. ***Participant Privacy Official*** means the individual appointed by Participant to oversee the privacy and security aspects of the implementation of the MX System and/or Services by Participant.

41. ***Participant Type*** means the category(ies) of Participant to which a particular Participant is assigned by MX based upon that Participant's role in the Healthcare system, as more specifically described in the Policies.

42. ***Participation Agreement or Agreement*** means a legally binding agreement between MX and a party pursuant to which that party acts in accordance with, and agrees to comply with the Participation Agreement and the Policies (and all references herein to the "Participation Agreement" shall incorporate by reference the Participation Agreement and the Policies, as amended, repealed and/or restated from time to time in accordance with the terms hereof andthereof).

43. ***Patient Data*** means health information that: (a) is created or received by a Healthcare Provider or Health Plan; (b) relates to: (i) past, present or future physical or mental health of a Patient, or (ii) the provision of health care to a Patient; (c) identifies the Patient, or there is a reasonable basis to believe the information can be used to identify the Patient (including Protected Health Information, as that term is defined in HIPAA, and Medical Information, as that term is defined in the CMIA); and (d) is made available to the System by a Participant pursuant to an Agreement.

44. ***Patient*** means each individual whose Patient Data is contributed to MX by a Participant.

45. ***Payment*** means the activities undertaken by (i) a Health Plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan or (ii) a Healthcare Provider or Health Plan to obtain or provide reimbursement for the provision of health care. Examples of payment are set forth in the HIPAA regulations at 45 C.F.R. § 164.501.

46. ***Payer Participant*** means a Health Plan, insurer or other payer Participant.

47. ***Permitted Purpose*** means one of the following reasons for which Participants or Participant Users may legitimately use Patient Data:
    1. Treatment, Payment, or Healthcare Operations pertaining to the individual who is the subject of the Patient Data, as permitted by the HIPAA Regulations;
    2. Public health activities and reporting as permitted or required by applicable Law, including the HIPAA Regulations at 45 C.F.R. § 164.512(b) or 164.514(e); and
    3.
    4. Uses and disclosures pursuant to an Authorization provided by the individual who is the subject of the Patient Data or such individual's personal representative as described in 45 C.F.R. § 164.502(g) of the HIPAA Regulations and in California Civil Code section 56.11(c).

48. ***Person*** means an individual person, an entity or a governmental organization or agency, including health information exchanges, and researchers, Participants and/or individuals who do not participate in MX's HIE.

49. ***Person of Public Interest*** means, at Participant's discretion, a person: (i) elected to State or Federal Office such as Congress, the Senate or the State Legislature; (ii) a Person who is appointed to serve in a Federal or State position of prominence; (iii) a nationally recognized entertainment figure; or (iv) any other person so designated by a Participant.

50. ***Personal Representative*** means a person who has the authority to consent to the disclosure of a Patient's/Member's Patient Data under any applicable Law.

51. ***PHI or Protected Health Information*** has the same meaning as the term is defined at 45 C.F.R. § 164.103.

52. ***Policies*** means, collectively, the privacy policies, security policies and/or procedural requirements adopted by MX, and made available to Participant, as amended by MX from time to time.

53. ***Primary Provider*** means a Healthcare Provider that is chosen by, assigned to or otherwise acts as a Patient's primary care provider for a Patient, acts as a gatekeeper for that Patient's medical care, is a credentialed provider, and who has a treatment relationship with the Patient. Most commonly

this is a Healthcare Provider whose name would appear in the clinical results as an ordering provider, attending provider, etc.

54. ***Provider Participant*** means hospitals, physicians, physician groups and other Participants that are not Payer Participants.

55. ***Readiness Assessment*** means the privacy and security assessment and review conducted by MX as part of the Application for Participation process.

56. ***Rescind the Opt-Out*** or ***Rescission of Opt-Out*** means a decision of a Patient/Member who previously executed an Opt-Out to rescind the Opt-Out and permit access to Patient Data relating to him or her through MX.

57. ***Research*** means a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge, including clinical trials, or as it may otherwise be defined at 45 C.F.R. § 164.501.

58. ***Successful Security Incident*** means a successful unauthorized penetration or compromise of the System's security (e.g., penetration of the firewall or other security mechanism) that does not result in access, use, receipt or disclosure of Protected Health Information, individually identifiable information, passwords, or user IDs.

59. ***Self-Pay Excluded Health Information*** means information in the records of a Healthcare Provider for which a patient has exercised his or her right under 45 C.F.R. § 164.522(a)(1)(vi)(B) to prohibit disclosures to a Health Plan of information relating to healthcare items or services for which the patient has paid in full out-of-pocket.

60. ***Services*** means the services provided by MX pursuant to a Participation Agreement.

61. ***Shared Healthcare Operations*** means the Healthcare operations for which covered entities may share Protected Health Information pursuant to 45 C.F.R. § 164.506(c) subsections (1) and (2).

62. ***System or MX System*** means the HIE and its related technology that MX provides to a Participant, as further described in these Policies and the Agreement.

63. ***Treatment*** means the provision, coordination or management of Healthcare and related services among Healthcare Providers or by a single Healthcare Provider, and may include providers sharing information with a third party. Consultation between Healthcare Providers regarding a patient and the referral of a patient from one Healthcare Provider to another also are included within the definition of Treatment. As used herein, uses and disclosures for Treatment purposes includes only those purposes permitted under 45 C.F.R. § 501 and Cal. Civ. Code § 56, *et seq*.

64. ***Unsecured Protected Health Information*** means Protected Health Information (as defined under HIPAA and HITECH) that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary of the U.S. Department of Health & Human Services (through guidance issued pursuant to HITECH).

65. ***Unsuccessful Security Incident*** means an attempted unauthorized access that did not penetrate or compromise the system security and does not result in access, use, receipt or disclosure of Protected Health Information, individually identifiable information, passwords, or user IDs.

66. ***User Authentication*** means the procedure established to assure that each Authorized User is identified by Participant's Administrator and the validity of such Authorized User's credentials is established by Participant's Administrator before such Authorized User is granted access to the MX System, in accordance with the MX requirements set forth in the policy, "Identification of Administrators And Authorized Users' Access to Data."

PP-1 MX POLICIES: OPENNESS, TRANSPARENCY AND PRIVACY

I. Policy

MX is committed to developing and maintaining a trust relationship with individuals whose PHI is shared through the MX System. MX will be open about its information-handling practices and will strive to maintain the highest levels of privacy and security in its operations. It will also require the same or higher standards of Participants and their Business Associates as a condition of their participation.

Openness about developments, procedures, policies, technology, and practices with respect to the treatment of PHI is essential to protecting privacy. Individuals should be able to understand what information exists about them, how it is used, and how they can exercise reasonable control over it. Transparency encourages a commitment to strong privacy practices and instills patient confidence in the privacy of their information, which in turn increases participation in the MX System.

II. Responsible Parties

This Policy applies to MX.

III. Procedural Requirements

A. MX has developed and adopted these Policies regarding information use, privacy, and security, as provided in the Participation Agreement, and may amend, repeal and/or restate the Policies in accordance with these Policies and the applicable Participation Agreement.

B. Policies shall be reviewed annually by the MX Privacy Officer and Security Officer.

C. In the event of a conflict between the Participation Agreement and the Policies, these Policies shall control.

PP-2 PARTICIPANTS

I. Policy

It is the policy of MX that only those Participants that execute a Participation Agreement may access the System.

II. Responsible Parties

This policy applies to MX and Participants.

III. MX Participation Requirements

Only persons who enter into Participation Agreements with MX shall be permitted to access the System and use the Services. A Participant may use the System and some or all of the Services in accordance with that Participant's Participation Agreement.

IV. Procedural Requirements

A. MX shall ensure that each person requesting to participate in the MX System indicates the type of entity it is as part of the process. Entities may include, but not be limited to, a) physician, medical group, or independent physician association; b) laboratory; c) hospital; d) public health agency; e) emergency medical services (EMS); f) pharmacy; health plan, insurer, or other payer; and g) business associates of any of the above.

PP-3 PARTICIPATION IN EXCHANGE FRAMEWORKS

I. Policy

MX seeks to provide the most comprehensive health information exchange functionality possible to its Participants, supporting: (1) access to the most robust data set possible for Permitted Uses; and (2) Participant compliance with information sharing requirements, including the Information Blocking Rule (45 CFR Part 171). As a result, MX may enter into agreements to participate in regional or national information exchanges or frameworks, which may include Carequality, eHealth Exchange, the Trusted Exchange Framework and Common Agreement (TEFCA), Patient Centered Data Home (PCDH), or other health information network, exchange, or framework as MX deems reasonable and appropriate.

Participant grants MX the right to provide Patient Data to Persons participating in Exchange Frameworks; provided, however, that MX may only make Patient Data available to such Persons in compliance with HIPAA and applicable Law.

II. Responsible Parties

This policy applies to MX and Participants.

III. Procedural Requirements

A. MX shall evaluate the security and policies of any exchange or network prior to joining and will only join those networks whose security requirements meet or exceed industry best practices.

B. If appropriate, MX may limit access to Participant data through Exchange Frameworks. An example of such a limitation would be to provide specific types of data, but not all Patient Data available through the System.

PP-4 PERMITTED USES OF DATA AND THE SYSTEM

I. Participants must comply with applicable Law related to the use and disclosure of Patient Data, as well as with the Participation Agreement and MX Policies governing the use and disclosure of Patient Data.

In the same way that Participants currently have the responsibility to safeguard Protected Health Information contained in their own records, they will have the same responsibility to safeguard Protected Health Information obtained through MX appropriately and to comply with the restrictions set forth in the Policies and in the Participation Agreement.

II. Responsible Parties

This Policy applies to MX and Participants.

III. Procedural Requirements

A. Internal Policies.

Participants and MX shall ensure through their individual internal processes that Healthcare Data obtained by an Authorized User or MX Personnel through MX may be used or disclosed by the Authorized User's or MX's Personnel only for the purposes permitted by the Participation Agreement and these Policies.

Participants and MX shall execute Business Associate Agreements binding any business associates accessing the System on their behalf to compliance with these Policies and the Participation Agreement.

In addition to the requirements herein, Participants shall refer to and comply with their own internal policies and procedures regarding use and disclosure of Protected Health Information and conditions that shall be met prior to making disclosures.

B. Minimum Necessary.

1. MX and each Participant will make reasonable efforts, except in the case of access for Treatment purposes, to limit information accessed through the MX System to the minimum amount necessary to accomplish the intended purpose for which it is being accessed.

2. During the process of identifying a Patient/Member and locating a Patient's/Member's LPR through a record locator service or other comparable directory, MX and each Participant will (i) implement safeguards to minimize unauthorized incidental disclosures of Patient Data, (ii) include the minimum amount of demographic information reasonably necessary to enable Authorized Users to successfully identify a Patient/Member through the record locator system, and (iii) prohibit, or restrict to the extent reasonably possible, Authorized Users from accessing Patient Data in any manner inconsistent with these Policies.

C. Role Based Access.

1. Participants who are Providers may only access data if needed for Treatment or Payment purposes as permitted by HIPAA. Health Plans may only access data for Members and consistent with Participant Policy 15.

2. With respect to Participants that are Health Plans, MX shall confirm the Patient's member/enrollee status through eligibility files supplied by each Health Plan or as otherwise permitted by MX's requirements for determining member/enrollee status. Any access of Patient/Member Data is subject to audit at MX's sole discretion to ensure that access was in accordance with these Policies and applicable Law.

D. MX Access.

1. Except as set forth elsewhere in the Policies, MX may only access and/or use Patient Data to:

   a. Acquire, aggregate, curate, analyze and manage Patient Data from Participants for the services MX is providing to Participants;

   b. Perform administrative tasks related to MX's business operations, as permitted by the Business Associate Agreement entered into between MX and Participants;

   c. On behalf of itself and Participants, comply with obligations required by applicable Law;

   d. Perform audits as permitted or required by applicable Law, including audits that test the functionality of the MX System, privacy audits to ensure that Patient Data is used and disclosed in accordance with the Policies, applicable Law, and the Participation Agreement; and investigations in response to reports of System failures or in order to improve System operations to avoid future System failures;

   e. Perform searches to harmonize duplicate medical records and ensure data quality, including validation of identities of Patients/Members for the purpose of compiling LPRs; and

   f. Carry out operations as required to implement Opt-Outs and Rescissions of Opt-Outs; and

   g. Engage in any other uses or activities that are permitted by Law and are not prohibited by a Participation Agreement or the MX Policies.

E. Permitted Purposes.

Participant and its Personnel may only use Healthcare Data for a Permitted Purpose in accordance with the Participation Agreement, these Policies and applicable Law.

F. Prohibited Purposes. Participants and their Personnel may not use Healthcare Data obtained from MX:

1. To publish or otherwise publicly disseminate any marketing comparisons of the performance of such Participant and/or other Participants without the express written consent of MX and each of the other Participants being compared; or

2. To strategize, argue or otherwise negotiate any Health Plan contract, or in any way to assist Participant in negotiating any contract or other commercial arrangement with another Participant, health care payer, hospital, physician or other health care provider.

G. Requirements for De-Identified Data.

1. MX may not Sell De-Identified Data.

2. MX and its Participants will subject any transfer or use of De-Identified Data to adequate restrictions to protect against re-identification of such data.

3. Any recipient of De-Identified Data shall agree in writing not to Sell or re-sell De-Identified Data or to combine it with other data in a manner that results in an identifiable data set.

4. "Sell" has the meaning given to it in 45 C.F.R. § 164.502(a)(5).

H. Access by Participant Applications. MX will permit Participant's Applications to access Patient Data through the MX System in accordance with the terms of these Policies and MX's published specifications for application programming interfaces or APIs.

I. Unauthorized Access and Use. Each Participant and its Personnel shall not: (i) attempt to gain unauthorized access to the Vendor Proprietary Information; (ii) alter or modify the underlying System, software, any vendor services agreement, API key, or Documentation (excluding training documentation); (iii) permit the Vendor Proprietary Information to be combined with any other programs to form a combined work, except to the extent reasonably necessary for a Participant's and/or its Authorized Users' access or use of that Vendor Proprietary Information; (iv) modify, enhance or create derivative works of the System or the Vendor Proprietary Information; (v) reverse engineer or otherwise attempt to derive the source code of the System or Vendor Proprietary Information; (vi) lease, sublease, sublicense, sell, distribute, transfer possession, rent, or grant other rights in the System, the Vendor Proprietary Information or the API key; or (vii) engage in service bureau work or time-sharing arrangements with respect to the System.

J. MX Malicious Software. MX shall use commercially reasonable efforts to ensure that no component of the System or Services includes any program, routine, subroutine, or data which: (a) will disrupt the proper operation of the System, the Services or any hardware, software or data used by a Participant in connection therewith; or (b) will cause the System, the Services or any hardware, software or data used by a Participant in connection therewith, to be destroyed, damaged, or rendered inoperable.

K. Participant Malicious Software. Each Participant shall use commercially reasonable efforts to ensure that: (a) no Patient Data includes, (b) Participant's connection to and use of the System does not include, and (c) Participant's method of transmitting that data will not introduce, any program, routine, subroutine, or data which: (i) will disrupt the proper operation of the System or any hardware, software or Healthcare Data used by MX or another Participant in connection therewith; or (ii) will cause the System, the Services, or any hardware, software or Healthcare Data used by MX or another Participant in connection therewith, to be destroyed, damaged, or rendered inoperable.

PP-5 PARTICIPANT ACCESS TO PATIENT DATA

I. Policy

It is the policy of MX to require Participants to identify a Participant Administrator. MX will grant Participant Administrators access to the System. In turn, Participant Administrator(s) will be responsible for identifying Participant's Authorized Users.

It is the policy of MX to appoint at least one MX Administrator. MX will grant MX Administrators access to the System. Such MX Administrators will in turn be responsible for identifying MX's Authorized Users.

It is the policy of MX that Authorized Users are only permitted to access and use Patient Data in accordance with the Participation Agreement, these Policies and applicable Law.

II. Responsible Parties

This Policy applies to Participants and MX.

III. Procedural Requirements

A. MX shall provide Participants a written protocol detailing the appropriate procedure for identifying Participant Administrators and Authorized Users, granting access to the System and/or the Services, and terminating access to the System and/or the Services. Participants shall appoint at least one Participant Administrator, and require each Participant Administrator to abide by the terms of this protocol. Access to Patient Data shall be restricted to Authorized Users only. The protocol shall include the following requirements:

1. <u>Identifying Participant Administrators.</u>

a. Participants shall submit the following required information to MX for each Participant Administrator: (i) first and last name; (ii) title and job function; (iii) office location; (iv) office and cell phone number; (v) office email address; and (vi) National Provider Identifier of Participant, if applicable.

b. Participants shall ensure that their respective Participant Administrator(s) are vetted through a background check screening process.

c. MX shall issue a username to each Participant Administrator.

d. Participant Administrator(s) shall agree to make reasonable efforts to ensure that Authorized Users act in accordance with these Policies and the Participation Agreement.

2. <u>Identifying Authorized Users.</u>

a. Upon MX's issuance of a username to Participant Administrator(s), Participant Administrator(s) shall identify Authorized Users who shall be

permitted to use the System and/or the Services in accordance with these Policies and the Participation Agreement.

b. As determined between Participant and MX, Participant Administrator(s) OR MX shall be responsible for providing a username, password and/or other security measure to the appropriate Authorized Users of Participant. The username and password shall be unique to each Authorized User; group or temporary usernames are prohibited.

c. The password assigned to each Authorized User must meet the password requirements as communicated by MX from time to time a MX deems appropriate to maintain the security of the MX System.

d. Participant Administrator(s) shall not permit Authorized Users to access the MX System unless a Participant Administrator receives a completed attestation (or an equivalent electronic certification, if so approved by MX) from each Authorized User that the Authorized User has completed the required Training, as further described in the policy entitled, "Training."

e. Access to PHI by Participants is based on defined roles or profiles. The following user profiles and descriptions are established in the MX System environment, and Participant Administrator(s) shall be responsible for reviewing and assigning one of the following roles to Authorized Users:

Level 1 – Primary Provider. This role will have access to clinical information, as permitted under HIPAA to support point of care clinical treatment. Examples include a physician, a nurse practitioner, care management staff and a medical resident.

- Access to all clinical views and reports
- Access to patient notifications

Level 2 – Secondary provider. Secondary providers work in conjunction with the Primary Provider in providing patient care. This person works under a fully licensed provider. Designed to access limited clinical content available within the CDR. This role will assume responsibility to access clinical content within the CDR to support point of care clinical treatment. Examples include nurses, interns, therapists or pharmacists.

- Access to all clinical views and reports
- Access to patient notifications

Level 3 – Auditor: will have access to utilization reports with the responsibility of monitoring reports and certain audit logs

Level 4 – Front desk/ back office: Designed to access only demographic data and opt out/in patients.

Level 5 –Administrator:

5.a – MX Administrator: Designed to support the global operational nature of providing user access controls and onboarding of users for the MX System. It is not intended to support point of care for clinical treatment.

- Access to user administration and auditing screens for the MX System

5.b – Participant Administrator: Designed to support the operational nature of providing user access controls and onboarding of the Participant's Authorized Users. It is not intended to support point of care for clinical treatment.

- Access to user administration and auditing screens for the Participant

Level 6 – Privacy Officer:

6.a. – MX Privacy Officer: Designed to support auditing capabilities with access to usability reports and basic configurations of the MX System. It is not intended to support point of care for clinical treatment.

- Access all patient administration screens to manage consent across the entire MX System

6.b. – Participant Privacy Officer: Designed to support auditing capabilities with access to usability reports and basic configurations of the Participant within the MX System. It is not intended to support point of care for clinical treatment.

- Access all patient administration screens to manage consent for the Participant.

Level 7 – EMPI user: Access for maintaining the EMPI (merge/unmerge potential duplications, keeping track of tuning, etc.).

f. Participant Administrator(s) shall ensure that the assignment of such roles remains accurate and appropriate to each Authorized User's job function and need for access, and shall re-assign user roles to Authorized

Users when necessary, such as when Authorized User's job function changes.

g. Participant Administrator(s) shall follow MX processes to request access for Participant Privacy Official and any other Authorized User who requires a higher level of access to the System.

h. Participant Administrator(s) shall notify MX promptly in the event of a job change or other event that requires removal of Participant Privacy Official or other higher level access to the System.

3. Access to the System and Services.

a. Participant Administrator(s) shall prohibit Authorized Users from sharing their usernames or passwords with others, and shall direct Authorized Users to only use their own usernames and passwords to log into the MX System.

b. Participant Administrator(s) shall utilize ID proofing and authentication methodologies that meets the minimum technical requirements for Identity Assurance Level 2 and Authentication Assurance Level 2 as set forth in National Institute of Standards and Technology Special Publication 800-63.

c. Participant Administrator(s) shall maintain a record of all Authorized Users and a copy of the Authorized User Confidentiality Agreement signed by each such Authorized User. Upon MX's request, the Participant Administrator shall provide a list in a medium and format requested by MX identifying all of Participant's Authorized Users and, if requested a copy of the Authorized User Confidentiality Agreement. MX shall have the right to audit the accuracy and completeness of that list and/or the Authorized User Confidentiality Agreements at any time and for any reason, and Participant Administrator shall assist MX in carrying out such audit.

d. Participant shall sanction Authorized Users who fail to act in accordance with the Participation Agreement, the Policies, or in accordance with the Participant's disciplinary policies and procedures and Participant shall notify MX as promptly as reasonably possible but in any event within 1 calendar day after Participant becomes aware that an Authorized User has violated or threatened to violate the Participation Agreement and/or Policies.

e. Access to Patient Data shall in all cases be restricted to Authorized Users only.

4. Terminating Access to the System and Services.

   a. Participant Administrators as well as MX shall have the right to terminate the credentials of Authorized Users.

   b. Authorized Users shall be immediately terminated by Participant if their employment or contract with Participant ends.

   c. MX shall have the discretion to require Participant to identify an alternate Participant Administrator(s) at any time.

   e. MX may require Participant to terminate or suspend an Authorized User's access to the System. For example, and not intending to limit MX's discretion to require termination in other circumstances, MX may exercise this discretion upon learning that an Authorized User has violated or threatened to violate the Participation Agreement and/or these Policies.

   f. Upon any termination of Participant's Participation Agreement, that Participant, its Participant Administrators and its Authorized Users do not have any rights to use the System or Services. MX shall ensure that access to the System and/or the Services shall be immediately terminated.

B. Designation and Responsibilities of MX Administrator(s).

1. MX shall appoint and issue a username to at least one MX Administrator who has been vetted through a background check screening process.

2. MX Administrator(s) shall identify MX Personnel who shall be permitted to use the MX System and/or the Services in accordance with these Policies and the Participation Agreement.

3. MX Administrator(s) shall be responsible for providing a username, password and/or other security measure to MX Personnel. A username shall be assigned to each MX Personnel; group or temporary usernames are not permitted. MX Administrator(s) shall activate and authenticate each MX Personnel's account in the MX System.

4. The password assigned to each MX Personnel must meet the password strength requirements set forth in National Institute of Standards and Technology Special Publication 800-63, and will require that MX Personnel change passwords at least every 90 calendar days, and prohibit MX Personnel from reusing the last six passwords.

5. Usernames and passwords must not be conveyed using any electronic method (including email) unless adequate security measures are taken to ensure that the usernames and passwords will not be intercepted or otherwise accessed by anyone other than the person to whom such usernames and passwords are intended to be conveyed.

6. MX Administrator(s) shall not permit MX Personnel to access the MX System unless the MX Administrator is satisfied that the required Training has been completed, as further described in the policy entitled, "Training."

7. MX Administrator(s) shall ensure that the assignment of user roles remains accurate and appropriate to MX Personnel's job function and need for access, and shall re-assign user roles to MX Personnel when necessary, such as in the event of when a job function changes.

8. MX Administrator(s) shall agree to make reasonable efforts to ensure that MX Personnel act in accordance with these Policies and the Participation Agreement, including prohibiting MX Personnel from sharing their usernames or passwords with others, and directing MX Personnel to only use their own usernames and passwords to log into the MX System.

9. MX Administrator(s) must utilize ID proofing and authentication methodologies that meets the minimum technical requirements for Identity Assurance Level 2 and Authentication Assurance Level 2 as set forth in National Institute of Standards and Technology Special Publication 800-63.

10. The MX System shall limit all users (both Participants and MX Personnel) to three consecutive Failed Access Attempts after which user's password shall be suspended.

11. The MX System will automatically log out all users (both Participants and MX Personnel) who are inactive after 15 minutes.

12. MX Administrator(s) shall maintain a record of all MX Personnel authorized to access the System.

13. MX Administrator(s) shall sanction MX Personnel who fail to act in accordance with the Participation Agreement, the Policies, or in accordance with MX's disciplinary policies and procedures.

14. Access to Patient Data shall in all cases be restricted to MX Personnel who have been properly issued MX System accounts.

15. MX Administrators shall have the right to terminate the credentials of Authorized Users and of MX Personnel.

PP-6 TERMINATION OF PARTICIPANT ACCESS TO PATIENT DATA

I. Policy

It is the policy of MX that upon termination of a Participant's participation in MX, whether such termination is initiated by the Participant or by MX, Participant's Patient Data may remain available to the remaining Participants through MX subject to the applicable terms of the Participation Agreement.

II. Responsible Parties

This Policy applies to MX and Participants.

III. Procedural Requirements

A. Access to Patient Data contributed by Participants is determined based on these Policies.

B. Upon termination of participation in MX, it will not be feasible for MX to return or destroy the Patient Data in the System.

C. MX will update its website and other materials in a timely manner to remove the name of the terminating Participant.

PP-7 OPT-OUT

I. Policy

It is the policy of MX that Patients/Members have the right to Opt-Out of having Patient Data about them accessible to Participants through MX. If a Patient/Member exercises his/her right to Opt-Out, the Patient/Member may Rescind the Opt-Out (and thereby have his/her Patient Data accessible) upon notification to MX.

II. Responsible Parties

This Policy applies to MX and Participants.

III. Procedural Requirements

A. Opt-Out

1. Each Participant shall develop and implement processes to inform its Patients/Members of their right to Opt-Out of having Patient Data about them accessible to Data Recipients through MX. A sample Privacy Notice is included as Appendix A.

2. The right to Opt-Out or Rescind the Opt-Out can be exercised by Patients/Members or persons legally authorized to act on their behalf.

3. MX may also provide Patient/Members with information about how they can exercise their right to Opt-Out or, if they have previously Opted-Out, their right to Rescind the Opt-Out.

4. A Patient/Member's failure to Opt-out results in being automatically included in MX. Patients shall make opt-out requests directly to MX. MX shall manage Patient/Member Opt-Outs, and ensure that access is blocked to a Patient/Member's data if that Patient/Member has Opted-Out of MX.

5. If a Participant or MX receives a Patient/Member's request asking that some but not all of his/her Patient Data be accessible through MX, then MX shall inform Patient/Member that any such restriction must apply to all of his/her Patient Data, i.e., all of his/her Patient Data will be inaccessible through the MX System.

6. A decision by a Patient/Member to Opt-Out only affects the accessibility of his/her Patient Data in the MX System.

7. In accordance with these Policies, each Participant will provide Patients/Members with: (i) notice – in a manner easily understood by Patients/Members – that their Patient Data is being exchanged through the MX System unless they affirmatively Opt-out; and (ii) a description of how Patients/Members may execute an Opt-out of having their Patient Data accessible through the MX System, or may potentially reverse this decision by executing a Rescission of Opt-out.

8. Patients/Members who have previously chosen to opt-out of the MX health information exchange, and who later wish to Rescind the Opt-out may do so at any time.

9. Opt-out is not retroactive as to information already released through MX, but it will restrict future exchange of Patient Data through the MX health information exchange.

10. Opt-out provisions are not applicable to Patient Data which providers or health plans share to support authorization of services to patients, where those patients have already been informed of such sharing by a provider or health plan Notice of Privacy Practices.

PP-8 INFORMATION SUBJECT TO SPECIAL PROTECTION

I. Policy

It is the policy of MX to comply with applicable Law.

It is the policy of MX to exclude from the System Patient Data that is (i) Excluded Health Information, (ii) Self Pay Excluded Health Information, and (iii) Data from Persons of Public Interest.

II. Responsible Parties

MX and Participants shall be responsible for compliance and implementation of this Policy.

III. Procedural Requirements

A. Excluded Health Information.

1. Participants shall not submit Excluded Health Information.

B. Self-Pay Excluded Patient Data.

1. If a patient has exercised his or her or her right under 45 C.F.R. § 164.522(a) (1) (vi) (B), Participants are solely responsible for excluding this data from MX.

C. Persons of Public Interest.

1. MX recognizes that Participants may provide treatment to persons they consider Persons of Public Interest. Participants may, at their sole discretion, choose to exclude this data from MX. Participants are responsible for determining whether Persons of Public Interest need to be notified that their data will not be accessible through the System and for providing this notification to those persons if necessary.

PP-9 DATA CONTRIBUTION

I. Policy

It is the policy of MX to require Participants to comply with all applicable Law, to reduce unnecessary risk to MX or its Participants that may be posed by certain data, to comply with any restrictions imposed by MX, third parties or Patient/Members and to provide consistent Patient Data to MX.

II. Responsible Parties

This Policy applies to MX and Participants.

III. Procedural Guidelines

A. Data Submission:

1. Participants that are Health Plans shall contribute Patient Data for individuals who are currently enrolled in the Health Plan.

3. Participants shall contribute data in accordance with the Participation Agreement and to the extent permissible by applicable Law

4. Participants are responsible for complying with all technical requirements set forth in the policy, "Participant Responsibility for System Support."

5. Participants must develop policies and procedures to verify the quality and integrity of the data they provide to MX.

B. MX Data Quality Responsibilities.

1. In the most expedient time possible and without unreasonable delay, MX, with the assistance of its Participants, shall investigate the scope and magnitude of any data inconsistency or potential error that was made by MX in the course of MX's data aggregation and exchange activities and, if an error is determined to exist, MX shall identify the root cause of the error and ensure its correction. MX shall log all such errors, the actions taken to address them and the final resolution of the error, and notify Participants where, in MX's judgment, such notification is reasonably necessary.

PP-10 PRIVACY OFFICER

I. Policy

It is the policy of MX that MX and Participants shall each designate an individual or individuals to oversee the access and use of Healthcare Data through the System and Services.

II. Responsible Parties

This Policy applies to MX and Participants.

III. Procedural Requirements

1. Privacy Official of MX is the Privacy Officer. MX Privacy Officer shall oversee all ongoing activities related to the development, implementation, maintenance of, and adherence to these MX's policies and procedures covering the privacy and confidentiality of Healthcare Data in compliance with the Participation Agreement, the Policies, and applicable Law.

2. Participant Privacy Official may vary with each Participant and may be at the Participant's discretion the same individual charged with overseeing the Participant's HIPAA compliance.

3. Participant Privacy Official shall oversee the implementation of the System and/or Services by the Participant and shall ensure the compliance of Participant, Participant Administrator, and Authorized Users with the Participation Agreement and the Policies.

PP-11 ACCESS, AMENDMENT, & ACCOUNTING OF PATIENT DATA

I. Policy

MX will assist, as set forth in this Policy, its Participant Covered Entities with complying with the requirements under HIPAA and HITECH for access to Patient Data, amendment of Patient Data and accounting for disclosures of Patient Data.

II. Responsible Parties

This Policy applies to MX and Participants.

III. Procedural Requirements

A. Any requests from Patients/Members for access to or amendment of their records shall be directed to the appropriate Participant for action. Response to individuals will be the responsibility of the Covered Entity Participant. MX shall within ten (10) days of the Covered Entity's request, cooperate with the Covered Entity, including providing access to the Patient/Member to a Patient/Member's PHI or incorporating any amendments to PHI that are directed by Covered Entity.

B. Any requests from Patients/Members for an accounting of disclosures shall be directed to the appropriate Participant. MX shall provide an accounting of disclosures, as defined under HIPAA, to Covered Entity Participant within ten (10) business days of a receipt of such request, to assist the Participant in meeting its responsibilities under 45 C.F.R. § 164.528. Covered Entity shall be responsible for providing all accountings of disclosures to Patients/Members, and MX shall not provide any accountings to Patients directly,

PP-12 SECURITY INCIDENT AND BREACH RESPONSE

I. Policy

It is the policy of MX that MX and Participants shall have staff identified and trained, and procedures in place for immediately investigating and mitigating, to the extent possible, any Successful Security Incident or Breach of Privacy or Security of which they become aware; and for reporting the Successful Security Incident or Breach of Privacy or Security to each other in accordance with the Participation Agreement.

It is also the policy of MX that Participants and MX shall cooperate with each other in the investigation and mitigation of any Successful Security Incident or Breach of Privacy and/or Security of which they become aware.

MX shall be responsible for reporting any Successful Security Incident or Breach of Privacy or Security of which MX becomes aware to each Participant affected by such Successful Security Incident or Breach of Privacy or Security, and for assisting Participants in the investigation and mitigation of any such Successful Security Incident or Breach of Privacy or Security in accordance with the terms of the Participation Agreement.

In addition, it is the policy of MX that Participants (in their capacity as a Covered Entity) are responsible for determining whether a Breach of Privacy or Security has occurred and whether notification of affected individuals in accordance with applicable Law is required, with the assistance of MX.

II. Responsible Parties

This Policy applies to MX and Participants.

III. Procedural Requirements

A. In the event Participant or MX becomes aware of a Breach of Privacy or Security or a Successful Security Incident within the System, notification will be made without unreasonable delay, within two business days of the Breach of Privacy or Security Successful Security Incident by (a) notification by Participant to MX's Privacy Officer; or (b) notification by MX to Participant's designated privacy contact person.

B. The notification should include sufficient information to understand the nature of the Breach or Successful Security Incident. For instance, such notification could include, to the extent available at the time of the notification, the following information:

1. One or two sentence description of the Breach or Successful Security Incident.

2. Description of the roles of the people involved in the Breach or Successful Security Incident (e.g. employees, Participant Users, service providers, unauthorized persons, etc.)

3. The type of Patient Data Breached or impacted by the Successful Security Incident.

4. Participants likely impacted by the Breach or Successful Security Incident.

5. Number of individuals or records impacted/estimated to be impacted by the Breach or Successful Security Incident.

6. Actions taken to mitigate the Breach or Successful Security Incident.

7. Current status of the Breach or Successful Security Incident (under investigation or resolved).

8. Corrective action taken and steps planned to be taken to prevent a similar Breach or Successful Security Incident.

C. The Participant or MX shall supplement the information contained in the notification as it becomes available and cooperate with other Participants.

D. In the event that MX discovers a successful Security Incident or Breach of Privacy or Security, MX shall, in addition to fulfilling the obligations set forth above, take immediate steps to mitigate the Security Incident or Breach of Privacy or Security, and MX shall then:

1. Investigate the scope and magnitude of the Successful Security Incident or Breach of Privacy or Security.

2. Identify the root cause of the Successful Security Incident or Breach of Privacy or Security.

3. Continue to mitigate the Successful Security Incident or Breach of Privacy or Security to the extent possible.

4. Provide a report of any Successful Security Incident or Breach of Privacy or Security including the root cause, analysis and corrective actions taken to the Board of Directors.

E. MX and each Participant shall comply with their respective reporting obligations to each other and, if applicable, to governmental authorities pursuant to their duties under applicable Law and their obligations under the Participation Agreement and/or BAA.

F. If, on the basis of the notification, MX determines that (i) the other Participants that have not been notified of the Breach or Successful Security Incident would benefit from a summary of the notification or (ii) a summary of the notification to the other Participants would enhance the security of the Performance and Service Specifications, it may provide, in a timely manner, a summary to such Participants that does not identify any of the Participants or individuals involved in the Breach or Successful Security Incident.

G. Cooperation with Audits. If Participant requires assistance with an audit by a Person (other than a Party) in connection with a Breach of Privacy or Security, MX shall: (a) use

commercially reasonable efforts to provide the information requested by the auditor; and (b) if requested by Participant, request assistance and cooperation from other Participants.

H. Cooperation with Audits. If MX or a Participant is audited by a Person in connection with a Breach of Privacy or Security and, related to that audit, reasonably requires information from Participant with respect to Patient Data provided by a Participant under the Agreement, then a Participant shall, at MX's request, cooperate with that audit and use commercially reasonable efforts to timely provide the information requested by MX for the audit. Any information provided to a Participant in connection with the audit will constitute Confidential Information of the other Participants, unless the other Participants indicate otherwise.

PP-13 COMPLIANCE WITH LAW

I. Policy

Participants shall comply with applicable law when submitting Patient Data to MX, and when Authorized Users or Applications access and/or use Data.

II. Responsible Parties

This Policy applies to Participants.

III. Procedural Requirements

A. Whenever a Participant submits Patient Data to MX, the Participant shall be responsible for:

1. Submitting Patient Data in compliance with applicable Law, the applicable Participation Agreement, and these policies and procedures; and

2. Ensuring that it has the requisite authority to make such a submission.

B. Whenever a Participant, including its Authorized Users, accesses Patient Data through MX, such Participant represents that the access is:

1. for a Permitted Purpose; and

2. Supported by appropriate legal authority for accessing the Patient Data.

C. Patient Data may contain PHI. Furthermore, some, but not all, Participants are either a Covered Entity or a Business Associate. Each Participant agrees as follows:

1. If the Participant is a Covered Entity, the Participant does, and at all times shall, comply with HIPAA to the extent applicable.

2. If the Participant is a Business Associate of a Covered Entity, the Participant does, and shall at all times, comply with the provisions of its Business Associate Agreements (or for governmental entities relying upon 45 C.F.R. §164.504(e)(3)(i)(A), its Memoranda of Understanding) and applicable Law.

3. If the Participant is a governmental entity, the Participant does, and at all times shall, comply with applicable Law, including but not limited to the applicable privacy and security Law.

PP-14 SANCTIONS

I. Policy

Sanctions are an important mechanism for ensuring that Participants and Authorized Users comply with these Policies. MX and its Participants will develop procedures to determine sanctions or disciplinary actions that may be imposed on a Participants and/or Authorized Users that fail to comply with these Policies.

II. Responsible Parties

This Policy applies to MX and Participants.

III. Procedural Requirements

A. MX will apply sanctions to Participants subject to the applicable terms of the Participation Agreement.

B. Each Participant shall apply sanctions to its Authorized Users in the event of violation of these Policies, or the Participation Agreement, in accordance with Participant's own internal disciplinary procedures.

1. Regardless of whether Participant applies disciplinary actions to its Authorized Users, MX retains the right to suspend or terminate an Authorized User's access if MX determines that the Authorized User's actions have, or are reasonably likely to, endanger the privacy, security or confidentiality of Patient Data, immediately upon written notice to the Participant.

C. MX will apply sanctions to MX Personnel in the event of violation of these Policies, or the Participation Agreement. Sanctions may include (i) requiring MX Personnel to undergo additional training with respect to participation in MX; (ii) suspending MX Personnel's access to the MX System; (iii) terminating the access of MX Personnel to the MX System; or (iv) termination or other disciplinary action taken in accordance with MX's applicable disciplinary procedures.

PP-15 TRAINING

I. Policy

It is the policy of MX to assure that in order to protect the welfare, safety and concerns of the Patients/Members whose Patient Data is stored in the MX System, all Authorized Users be aware of the privacy and security obligations of Participants and be trained in the appropriate use of the MX System.

It is also the policy of MX to train MX's Authorized Users in the appropriate use of the System and the privacy and security obligations of MX.

II. Responsible Parties

This policy applies to MX and Participants.

III. Procedural Requirements

A. To ensure Training of all Authorized Users:

1. MX shall develop Training for individuals who wish to become Participant Administrators or Training Coordinators. The Participant Administrators or Training Coordinators shall train that Participant's Authorized Users. Training will provide instruction and guidance as to the use of the MX System and Services only and functions as a complement, not a substitute, for Participant's existing privacy & security training for employees;

2. Participants shall only allow individuals who have completed the Training to access the MX System and/or Services. Participants shall require all Authorized Users to complete initial Training upon hire and annual refresher Training thereafter;

3. Inform Participants about the content and manner of Training, including who should be trained and how often such Training is required;

4. Periodically review the Training content for quality and implement corrections and improvements as needed;

5. MX shall provide ongoing Training for Participant Administrator on upgrades and enhancements to the MX System resulting from new releases of software and the availability of new types of Patient Data;

6. MX shall collect documentation from each Participant indicating that its Authorized Users have completed annual refresher Training and in its sole discretion audit Participants and/or ask Participants to provide additional documentation to verify that Authorized Users have completed their annual refresher Training; and

7. MX shall support each Participant Administrator as needed to address and resolve administrative issues relating to the Training program.

B. To ensure initial and annual refresher Training of its Authorized Users, Participants shall:

1. Arrange for and coordinate the initial Training of designated individuals to become Authorized Users or Participant Administrators;

2. Ensure that Participant Administrators arrange for activation of the accounts of Authorized Users who have completed the necessary Training programs on the Participant's local system;

3. Arrange for and coordinate the scheduling for Authorized Users to complete annual refresher Training; and

4. Verify, track and report that initial and annual refresher Training have been completed for each Authorized User. Specifically, Participant shall maintain reports identifying who completed the Training.

PP-16 DATA AND PHI ACCESS

I. Policy

Participants and MX will collaborate with each other in any environment that contains Protected Health Information ("PHI"), consistent with the procedures and administrative requirements that are described in this policy.

II. Responsible Parties

This policy applies to MX, MX Personnel and Participants.

III. Procedural Requirements.

A. Payer Participants that have executed a Participation Agreement with MX shall adhere to the following policies and procedures regarding data submission, access, viewing, use, and disclosure:

1. Payer Participants shall only view, access, use, or disclose Patient Data of current members or enrollees and shall not view any Patient Data, including PHI of individuals who are not current members or enrollees of that Participant;

2. Payer Participants shall maintain up-to-date membership files in MX. For purposes of this policy, an "up-to-date membership file" is a file that has been updated within the past 30 calendar days. Payer Participants may submit membership file updates more frequently;

3. Payer Participants shall use their internal current membership data files to identify members or enrollees whose Patient Data may be viewed, accessed, used, or disclosed through MX, and Payer Participants shall not view, access, use, or disclose Patient Data, including PHI, of any other individuals;

4. Each Payer Participant is responsible for reviewing all available information promptly to verify that any members or enrollees whose PHI was accessed by that Participant's Authorized Users are current plan members or enrollees of the Participant as of the date of viewing, access, use, or disclosure of Patient Data; and

5. Any Payer Participant that violates this policy by accessing, viewing, using, or disclosing PHI to any individual other than a current member or enrollee of that Participant is responsible for and shall timely conduct and pay for all state and federal breach reporting actions related to such access, viewing, use, or disclosure of such PHI or Patient Data.

B. Provider Participants shall only view, access, use, or disclose Patient Data for treatment or payment reasons as permitted by HIPAA.

PP-17 GENERAL PARTICIPANT SECURITY REQUIREMENTS

I. Policy

It is the policy of MX to collaborate with Participants in any environment that contains Protected Health Information ("PHI"), pursuant to the procedures and administrative requirements that are described in this policy.

II. Responsible Parties

This policy applies to MX, MX Personnel, and Participants.

III. Procedural Requirements

A. Identification. Each Participant shall employ a process by which the Participant, or its designee, validates sufficient information to uniquely identify each person seeking to become an Authorized User prior to issuing credentials that would grant the person access to the participant's system.

B. Authentication. Each Participant shall employ a process by which the Participant, or its designee, uses the credentials issued by MX to verify the identity of each Authorized User prior to enabling such Authorized User to transact message content.

C. General. Each Participant shall be responsible for maintaining a secure environment that supports the operation and continued development of the performance and service specifications. Participants shall use appropriate safeguards to prevent use or disclosure of message content other than as permitted by these policies, including appropriate administrative, physical, and technical safeguards that protect the confidentiality, integrity, and availability of that message content as required by the HIPAA security rule. Appropriate safeguards for federal Participants shall be those required by applicable law related to information security. Each Participant shall, as appropriate under either the HIPAA regulations, or under applicable law, have written privacy and security policies in place by the Participant's respective effective date. Participants shall also be required to comply with any performance and service specifications or operating policies and procedures adopted by MX that define expectations for Participants with respect to enterprise security.

D. Malicious software. Each Participant shall ensure that it employs security controls that meet applicable industry or federal standards so that the information and message content being transacted and any method of transacting such information and message content will not introduce any viruses, worms, unauthorized cookies, Trojan horses, malicious software, "malware," or other program, routine, subroutine, or data designed to disrupt the proper operation of a system or any part thereof or any hardware or software used by a Participant in connection therewith, or which, upon the occurrence of a certain event, the passage of time, or the taking of or failure to take any action, will cause a system or any part thereof or any hardware, software or data used by a Participant in connection therewith, to be improperly accessed, destroyed, damaged, or otherwise made inoperable. In the absence of applicable industry standards, each Participant shall use all commercially reasonable efforts to comply with the requirements of this policy.

E. Equipment and software. Each Participant shall be responsible for procuring, and assuring that its Authorized Users have or have access to, all equipment and software necessary for it to transact message content. Each Participant shall ensure that all computers and electronic devices owned or leased

by the Participant and its Participant users to be used to transact message content are properly configured, including, but not limited to, the base workstation operating system, web browser, and internet connectivity.

F. Auditing. Each Participant represents that, through its agents, employees, and independent contractors, it shall have the ability to monitor and audit all access to and use of its system related to this agreement, for system administration, security, and other legitimate purposes. Each Participant shall perform those auditing activities required by the performance and service specifications.

PP-18 PHYSICAL SECURITY

I. Policy

It is the policy of MX that appropriate physical security will be maintained by MX and Participants for all facilities and hardware in connection with the System.

II. Responsible Parties
This Policy applies to MX and Participants.

III. Procedural Guidelines

A. MX and Participants will comply with all applicable Laws and industry practices regarding system security, including meeting the standards established under HIPAA pertaining to workstation security.

B. MX will comply with the following physical security requirements:

1. To protect the confidentiality, integrity and availability of the System by taking reasonable steps to secure office and data center facilities from unauthorized physical access, tampering and theft and to locate System hardware where physical access can be controlled in order to minimize the risk of unauthorized access.

2. To operate the System on computers located in physically secure data center facilities with appropriate environmental, safety, and site security procedures, data security practices and other safeguards against the destruction, loss, alteration, or unauthorized access to the System and/or the data.

3. To establish and document detailed rules to determine which workforce members are granted physical access rights to specific areas where the System is maintained and to limit such physical access rights to workforce members having a need for access to the System and/or the data.

4. To limit access to work areas by visitors and to maintain a log of all authorized visitors.

5. To take reasonable steps to ensure that the level of protection provided by the System, as well as the facilities in which they are housed, is commensurate with that of identified threats and risks analyses in order to assess risk and adjust security controls and procedures accordingly.

C. MX and each Participant shall establish and maintain an information security program in order to implement the necessary controls and comply with this policy.

PP-19 SYSTEM SECURITY

I. Policy

It is the policy of MX that appropriate network and application security will be maintained by MX and Participants to protect the System from Security Incidents, unauthorized access, and Breaches of Privacy or Security.

II. Responsible Parties

This policy applies to MX and Participants.

III. Procedural Requirements

A. MX and Participants will comply with all applicable Laws and industry practices regarding system security, including meeting the standards established by HIPAA pertaining to system and workstation security.

B. MX and Participants will comply with the following security requirements:

1. Shall install, maintain and update on all of its computers used for the purpose of accessing the System virus protection software that is currently supported by the manufacturer and that automatically updates no less than once per week.

2. Shall install, maintain and update on all of its computers used for the purpose of accessing the System firewall and disk encryption software that is currently supported by the manufacturer and automatically updates no less than once a week.

3. Shall be responsible for ensuring that all computers including to their operating system and web browser used to access the System are currently supported by the manufacturer and properly configured and updated.

4. Shall implement safeguards to minimize unauthorized incidental disclosures of Patient Data during the process of identifying a Patient/Member and locating or matching his/her records.

C. Each Participant shall adopt and implement any security policies and procedures relating to the use, maintenance and disclosure of Patient Data obtained through the MX System that is necessary to ensure Participant's compliance with applicable Law.

D. MX and its vendors shall comply with the following system security requirements:

1. Store Patient Data on secure computers located in a secure data center(s) and shall establish, maintain, and comply with environmental, safety, and facility procedures, data security practices and other safeguards against destruction, loss, alteration, or unauthorized access or disclosure of Patient Data in its possession;

2. Employ technology that is consistent with industry standards for firewalls and other security technology to help prevent the Systems from being accessed by unauthorized persons including: (i) the use of HTTPS or equivalent standard for all browser access to Patient Data; (ii) ensure that all Patient Data is encrypted while in transmission or at rest;

(iii) MX shall use no less than 128 bit encryption technology for all Patient Data; (iv) provide the ability to transfer files via secure means (e.g., secure FTP);

3. Perform commercially reasonable monitoring of the System for health and performance, and shall have engineers available on-call to resolve any system issues;

4. Dispose of all electronic media that stores information in accordance with media sanitization standards established by NIST; shall retain records that identify the media disposed of including serial number of the unit and the media, if a serial number is available, the method of sanitization or destruction, and the date the media was disposed of; and

5. Take reasonable steps to ensure that the level of protection provided for the System is commensurate with that of the identified threats and risks to security of the System, MX shall perform a periodic risk analysis to assess the level of controls and procedures accordingly.

E. MX and each Participant shall establish and maintain an information security program in order to implement the necessary controls and comply with this policy.

PP-20 AUDIT POLICY AND PROCEDURAL REQUIREMENTS

I. Policy

It is the policy of MX to maintain routine audit logs of the accesses of Patient Data by the Authorized Users of Participants.

It is the policy of MX to audit its own uses and disclosures and to require that all Participants participate in audits on a reasonable basis in order to ensure that the MX System is being used only for purposes authorized by the Participation Agreement and these Policies, and that each Authorized User who views data through the MX System is doing so in a manner consistent with the Participation Agreement and these Policies, including those policies relating to privacy.

In addition, it is the policy of MX to require that all Participants cooperate with MX and/or other Participants with respect to any audits.

II. Responsible Parties

This Policy applies to MX and Participants.

III. Procedural Guidelines

A. Access Audits

1. The MX System will automatically record and log each access to Patient Data and will maintain these records for a period of at least six years from the date on which the information is accessed. Audit Logs of a Participant's Authorized Users will be made available to the Participant's Privacy Official upon request. Such Audit logs will track user access, including the patient name, data/time of record access, and type of data elements accessed.

2. MX shall prepare an audit schedule establishing timeframes for periodic, regular audits at a frequency deemed reasonable by MX and consistent with applicable Law.

3. If a Participant accesses Patient Data through an Application, the audits described above shall include access by each Authorized User through the Participant's system.

4. If any audit conducted by a Participant or MX identifies non-compliance with the Participation Agreement or any of these Policies or the Participation Agreement, then: (a) the party identifying the noncompliance will notify the responsible entity; (b) in the case of MX, MX will implement a corrective action plan; and (c) in the case of a Participant, the Participant will submit a corrective action plan to MX along with the audit report.

5. Depending on the nature of the problem uncovered in the audit, MX may suspend access to the MX System for either the Participant or one or more Authorized Users of such Participant until the problem is adequately addressed, in accordance with the procedures set forth for suspension in the Participation Agreement. Rights to suspend a Participant, an Authorized User of Participant,

or to terminate a Participation Agreement in the event of breach are covered in the Participation Agreement and the Business Associate Agreement.

6. MX will provide Participants, upon request and as promptly as reasonably practicable, information relating to data access or audit logs of any Patient/Member of the Participant whose Patient Data was accessed through the MX System.

B. Audits in Response to Inappropriate Activities. If MX has reason to believe that inappropriate accesses, uses, or disclosures of Patient Data are occurring by Participant, Authorized Users, or Participant Administrators, MX shall, at its discretion, perform an audit or require Participant to perform an audit to investigate the potential inappropriate accesses, uses or disclosures of Healthcare Data.

C. Audits by Third Parties. If Participant is the subject of a third-party audit related to Breach of Privacy and Security, and the auditor reasonably requires information regarding certain Patient Data provided to MX by a Participant, in accordance with the Participation Agreement, MX shall facilitate forwarding the Participant's request to the appropriate Participant to provide the information requested by the auditor.

D. Audits of Authorized User Protocols. In accordance with the Participation Agreement, MX may audit Participant's compliance with the protocols setting forth the identification of Authorized Users at any time and for any reason.

PP-21 PARTICIPANT RESPONSIBILITY FOR SYSTEM SUPPORT

I. Policy

It is the policy of MX that each Participant is responsible for maintaining internet and internal network connectivity and providing such other system support services as may be necessary to: (i) transmit Participant's data to the System; (ii) provide online access to the System; (iii) cooperate with MX in maximizing the performance and availability of the System for Participant's Authorized Users.

II. Responsible Parties

This Policy applies to all Participants.

III. Procedural Requirements

A. In addition to other obligations of Participants related to System support set forth in the Participation Agreement and these Policies and Procedures, each Participant is responsible for:

1. Maintaining internet and internal network connectivity and for the performance of the MX System as limited by that connectivity.

2. Adding MX domain names to access control or other security systems to permit access from Participant's network.

3. Providing the first level of support to its Authorized Users relating to access to and performance of the MX System that can then be escalated, if necessary, to MX's Help Desk.

4. Cooperating with MX's support personnel in troubleshooting any incidents experienced by Authorized Users with respect to access to and performance of the System.

5. Designating privacy officials and security administrators who will provide access to appropriate Authorized Users as set forth in the policy, "Identification of Administrators and Authorized Users' Access to Data."

6. Cooperating as reasonably necessary and at reasonable times with MX and its vendors in testing and implementing upgrades to the MX System.

B. In addition to the responsibilities set forth above, Participants are responsible for complying with the requirements set forth below. A Participant is also responsible for complying with the following, as specified in and adopted in substantially similar form by the agreement adopted by the Participant and MX:

1. Monitoring data feeds from its computer systems to the System and addressing any problems that may arise with respect to such data feeds, ensuring accurate and complete loading of clinical data from its computer systems to the System.

2. Notifying MX of any problems in the regular feeds of data to the System.

3. Ensuring the appropriate change management processes are in place to minimize any changes to its computer systems or operating systems.

4. Notifying MX of system changes that may require an update to the System so that MX can provide a statement of work for its changes and can participate in modification and/or testing procedures.

5. Monitoring connectivity to the System and coordinating with MX support services in accordance with the escalation process developed by MX as necessary to troubleshoot and resolve any problems or issues.

6. Following MX's procedures or processes for escalation of any problems/issues that arise with maintenance or use of the System that cannot be resolved locally.

7. Cooperate with MX to perform data quality analyses to determine whether data in the System accurately reflects the current data from Participant's system.

8. Cooperating with MX to investigate and resolve any operational issue identified by MX and communicated to the Participant.

9. Notify MX of any modifications or amendments to Patient Data as may be requested by the Member/Patient and which may be granted in compliance with applicable Law.

PP-22 OFFSHORE ACCESS

I. Policy

It is the policy of MX to limit Offshore access to the MX System and to only store Data in the United States.

II. Responsible Parties

MX and Participants are responsible for complying with this Policy.

III. Procedural Requirements

A. MX shall not allow Offshore access to PHI by MX Personnel, unless otherwise permitted by the Business Associate Agreement, except thatMX Vendors may access PHI from an Offshore location to provide engineering support to the System, which may include incidental access to PHI.

1. MX shall limit MX Vendors' Offshore access to PHI to that incidental access.

2. Prior to accessing PHI Offshore, MX Vendor shall provide Privacy and Security training to those employees, and shall deliver to MX a list of all MX Vendor employeeslocated Offshore who will have access to PHI, and shall deliver an update of thatlist whenever it changes.

B. Participants and/or their Business Associates shall not access the System from Offshore locations.

C. MX shall not store Data outside the United States without the prior written consent of Participants and in accordance with the applicable Business Associate Agreement.

PP-23 COMMITTEES

I. Policy

It is the policy of MX that it may establish advisory committees ("Advisory Committees"), the members of which may include Participants (including representatives from hospitals, physician groups and health plans), consumers, government employees and others involved in the delivery of healthcare, to advise MX on services, technologies, policies, privacy and other matters.

II. Responsible Parties

This Policy applies to MX and all Participants.

III. Procedural Requirements

C. Advisory Committees.

1. Establishment. MX has developed a governance model that includes an Advisory Committee to provide recommendations and input to MX senior leadership on key issues and decisions including product and services offerings, privacy and security policies, technology decisions and optimizing clinical value. The Advisory Committee is intended to be broad based to ensure that perspectives from a broad range of MX's diverse of stakeholders and Participants are represented. MX, in coordination with the Advisory Committee, may from time to time constitute topically focused subcommittees, which may include:

    i. Policy Subcommittee

    ii. Technology Subcommittee

    iii. Clinical Subcommittee

2. Responsibilities. Responsibilities of the Advisory Committee and each Subcommittee will be defined and maintained in specific committee charters.

3. Nomination and Appointment. MX solicits committee nominations from a wide range of stakeholders. All nominees must have subject matter expertise and/or experience and/or represent a key constituency in the MX service area. Each

MX-Affiliated HIO will have one seat on the Advisory Committee. Nominations must include the following information:

i. Nominee name

ii. Current position held

iii. Organization

iv. Areas of expertise

v. Current CV, including all organizational, professional or advisory positions

vi. A brief description of the candidate's qualifications to serve on the committee

MX staff will compile all nominations and evaluate candidates based on subject matter expertise and experience. MX senior leadership will appoint individuals to the Advisory Committee and Subcommittees, selecting from among those who have been nominated, aiming for the most capable team possible, while also seeking to ensure geographic and organizational diversity. Decisions made by the MX senior leadership will be final.

4. Term of Service. Advisory committee members will serve a one year term, with the possibility of annual reappointment by MX senior leadership without re-nomination for up to three additional successive one year terms. MX will not reappoint any committee member who expresses a desire to discontinue serving on The Advisory Committee or who has not actively participated in The Advisory Committee. In addition, Advisory Committee members may be removed at any time for material breach of applicable MX Policies and Procedures, including but not limited to conflicts of interest and confidentiality, as determined by MX senior leadership. At the conclusion of the fourth year of service, members will not be eligible for an annual reappointment vote and must be formally nominated again. Service will be uncompensated. All Advisory Committee work products will be the sole property of MX.

Appendix A - SAMPLE PRIVACY NOTICE AND OPT-OUT FORM FOR PARTICIPANTS (updated Jan 2020)

Sample Privacy Notice for Manifest MedEx Health Information Exchange

The purpose of this Notice is to advise you that the Manifest MedEx Health Information Exchange (MX) may facilitate electronic sharing of your personal health information among your healthcare providers in order for your medical treatment to be based on as complete a record as possible.

What is a health information exchange?

MX is a health information exchange. [PROVIDER] is a Participant in MX. MX facilitates the electronic transfer of protected health information among participating healthcare providers. MX houses and stores data in a secure environment and also makes the exchange of healthcare data among participating healthcare providers possible.

What information about you will be disclosed through MX?

To the extent permitted by law, [PROVIDER] may disclose your protected health information to other healthcare providers and health plans who request that information via the Exchange. Protected health information in this case includes information that has been created or received by a healthcare provider, which relates to your past, present or future mental or physical condition, and that is personally or individually identifiable as belonging to you.

In cases where your specific consent or authorization is required to disclose certain health information to others, [PROVIDER] will not disclose that health information to other healthcare providers or health plans participating in MX. Sensitive information that requires your additional consent in order to be shared includes; psychotherapy notes, treatment for substance or alcohol abuse and records of HIV tests.

Who may access information through MX?

Only Participants in the exchange who are your healthcare providers or health plans in which you are enrolled may access information through the Exchange.

For what purposes can such information can be accessed?

Information may be accessed for the purpose of your medical treatment, payment, and certain healthcare operations as permitted by federal and California privacy law.

Can you request your medical records and/or an accounting of disclosures of who has received them?

You may access your records or obtain information about who has requested or received them by making a written request to [PROVIDER] to release such data to you in accordance with [PROVIDER]'s policies.

Can you opt-out of sharing your protected health information with your healthcare providers via MX?

You have the ability to opt-out of sharing your PHI through the MX system. Please see the information about opting-out below.

If you do not opt-out of sharing protected health information with your other healthcare providers by way of the Exchange, then your consent to such sharing is assumed.

If you do NOT wish to allow your healthcare providers and health plan to share your protected health information electronically with each other via the Exchange, you may exercise your right to opt-out. The effect of opting-out of the Exchange is that each healthcare provider or health plan will need to request that a copy of your record be transferred by other means, such as by fax.

Opt-out provisions are not applicable to Patient Data which providers or health plans share to support authorization of services to patients, where those patients have already been informed of such sharing by a provider or health plan Notice of Privacy Practices.You may not be denied treatment or enrollment in a health plan or otherwise penalized if you opt-out of sharing your protected health information through MX.

If you opt-out of sharing your protected health information via MX and change your mind, you may opt back in at a later date. All health information collected during the opt-out period will be visible upon opt in.

Your participation in MX is voluntary and you may opt-out at a later date. If you choose to opt-out at a later date, data that has already been shared through MX will not be recalled from the provider(s) who have already received it, but no new data will be shared by MX.

See MX Opt-Out form https://www.manifestmedex.org/opt-out-2/ or complete the form online at https://www.manifestmedex.org/opt-out.

MX alternate suggested language for Notice of Privacy Practices:

[PROVIDER] is a Participant in Manifest MedEx (MX), a Health Information Exchange that facilitates the electronic sharing of health information between healthcare providers to support better informed, safer healthcare. You may choose not to have your health information shared through MX by opting-out. However, doing so means MX will not make your health information available to **any** healthcare providers, even in circumstances of emergency. If you would like to opt-out of MX, please complete and submit the online opt-out form at https://www.manifestmedex.org/opt-out or call 1 (800) 490-7617.

[optional to include] Opt-out provisions are not applicable to Patient Data which providers or health plans share to support authorization of services to patients, where those patients have already been informed of such sharing by a provider or health plan Notice of Privacy Practices.