Sample PMP Gateway Compliance Manual

MAPS – EHR Integration Initiative Resource

Michigan's updated and more user-friendly Michigan Automated Prescription System (MAPS), powered by the Appriss PMP AWARxE software platform, offers the option to integrate with users' electronic health records (EHRs). The goal is to increase the utilization of MAPS data within the clinical workflows of prescribers and pharmacists. Integration will enable hospitals, physicians, and pharmacists to have direct access to MAPS data without having to log out of one system and into another.

To participate:

1. Go to the Michigan Department of Licensing and Regulatory Affairs (LARA) webpage at http://www.michigan.gov/lara/0,4601,7-154-72600-424267--,00.html where you can access the Integration Request Form and the Terms and Conditions document.
2. Fill out the one-page Integration Request Form.
3. Review and sign the Terms and Conditions document.
4. Email the Integration Request Form and Terms and Conditions document to LARA at BPL-MAPS@michigan.gov.

Once your application is received, the State will notify Appriss Health. Appriss Health will then connect with your EHR vendor. It is also our understanding that you will be notified that your application has been received and that the LARA MAPS support team will be checking in to determine whether you have been contacted by Appriss Health or your EHR vendor regarding the integration.

One of the provisions in the **Terms and Conditions** document noted above, requires practices to have **policies and procedures** in place to ensure appropriate access, use, and security. MSMS Legal Counsel created the attached **template language** for practices to use as a guide to comply with this requirement.

Visit www.msms.org/BeAWARE under the "MAPS" header for additional information on the MAPS-EHR integration initiative.

Practice Name:

Effective Date:

Introduction

[Insert Practice Name] (the "Practice") contracts with the Michigan Department of Licensing and Regulatory Affairs ("MLARA") to allow authorized users to access and use its PMP Gateway Service for purposes of obtaining prescription history information ("PMP Data") maintained by one more state prescription monitoring programs ("PMPs"). MLARA requires the Practice and its Authorized Users (defined below) to fulfill specific PMP Gateway Service compliance requirements, which are described in this Manual.

Policy to Comply with Applicable Laws

It is the Practice's policy to comply with all local, state and federal laws and rules applicable to PMPs, PMP Data, personally identifiable information, and health information organizations, including, but not limited to, confidentiality, security, registration and licensure requirements, as well as all rules issued by Appriss, Inc., the PMP Gateway Service provider ("Service Provider"). The Practice likewise requires its Authorized Users to commit themselves and agree to comply with all applicable laws and rules.

Authorized Users must attest to compliance with applicable laws and requirements described in this Manual. The Practice will supply an attestation document for Authorized Users to sign and return to the Practice.

Who is an Authorized User?

An "Authorized User" means a validly licensed pharmacist or health care practitioner within the Practice's organization or a health care entity which has a member or client relationship with the Practice, as described in a valid agreement between the practitioner or entity and the Practice, authorized by the Practice to access PMP Data in accordance with applicable law.

Access and Use of PMP Gateway Service

Only an Authorized User may access or use the PMP Gateway Service. Authorized Users may only access or use the PMP Gateway Service and its systems used in connection therewith in a secure manner in accordance with applicable law and MLARA requirements. Authorized Users must be appropriately credentialed and validated as required under all applicable state and federal laws and rules and requirements for credentialing and validation of pharmacists, health care practitioners or entities who seek to access or use the Gateway Service or service information.

Permitted Access or Use:

Access or use of PMP Data or data that is input, transmitted or output via the PMP Gateway Service (e.g., user data, search criteria, PMP Data, etc.)("Service Information") shall be for the purpose of health care decision-making related to a specific patient encounter, in accordance with applicable law. Authorized Users shall limit any request, use or release protected health information ("PHI") to the minimum necessary amount to accomplish the purpose of the use, disclosure or request.

The Practice and its Authorized Users may not receive, create, use or disclose protected health information or confidential information except as follows:

- To facilitate the transmission of PHI from the PMP to the Practice in accordance with MCL §333.7333a; or
- If necessary for the proper management and administration of the Practice or to carry out legal responsibilities of the Practice. PHI may only be disclosed to another person/entity for such purposes if (1) disclosure is required by law; or (2) to the extent such disclosure is in compliance with privacy and security laws (including, but not limited to, the Health Insurance Portability and Accountability Act ("HIPAA") and the rules promulgated thereunder, as amended), MCL §333.7333a, as amended, and Michigan Board of Pharmacy Administrative Rules 338.3162b – 338.3163e, as amended.

The Practice and its Authorized Users Authorized Users must properly authenticate to the applicable PMP, as required, when seeking to query one or more state's PMPs.

Prohibited Conduct:

It is the Practice's policy that the Practice and each of its employees, agency, contractors, affiliates and Authorized Users will not engage in unlawful, objectionable, or malicious conduct or activities related to the PMP Gateway service, the PMP Gateway Service servers, or Service Information. Prohibit Conduct includes, but is not limited to:

- The transmission or distribution of viruses, computer worms, Trojan horses, malicious code, denial of service attacks, unsolicited commercial email, or the like;
- The unauthorized entry to any other machine accessible via the PMP Gateway Service;
- The unauthorized submission or transmission of data or material protected by a proprietary right of a third party; or
- The submission of otherwise objectionable information, material or communications.

Training:

It is the policy of the Practice that Authorized Users complete training on accessing and using the PMP Gateway Service provided by the Practice. The Practice shall maintain evidence of training completion as determined by the Practice.

Reporting and Investigation

It is the Practice's policy and requirement that suspected or detected non-compliance is to be reported to the Practice. All reports will be kept confidential to the extent reasonably possible.

The Practice will promptly investigate any complaint or report that a Practice employee, agent, contractor, affiliate or Authorized User failed to comply with any applicable law, rule or requirement for access or use of the PMP Gateway Service. The Practice holds individuals and entities responsible for violations of the Practice's policies or illegal acts. The source of any allegation of wrongdoing, whether an email, telephone or in person report, or any other source, is irrelevant to the Practice's obligation to investigate. The Practice will conduct all investigations in a manner that protects the rights of those who may be the subject of allegations of wrongdoing as well as those who, in good faith, make such allegations.

The Practice is required to promptly report the results of its investigation to MLARA, Michigan's PMP and any requesting state.

Incident Reporting, Remediation

Incident Reporting:

It is the Practice's policy to report to MLARA (1) any use or disclosure of PHI which is not in compliance with applicable laws, rules or requirements of which it becomes aware; and (2) any security incident of which it becomes aware. A "security incident" means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. Within 24 hours of discovery of a suspected reportable incident, the Practice shall notify MLARA of the existence and nature of the incident as understood at that time and immediately investigate the incident.

Within 72 hours of discovery of the incident, the Practice will provide MLARA a written report describing the results of the Practice's investigation. The report will be based on best available information known at the time. If the investigation is ongoing, the report should reflect that. The report must include the following information:

- What data elements were involved, the extent of the data involved in the incident, and the identification of affected individuals, if applicable;
- A description of the unauthorized persons known or reasonably believed to have improperly used or disclosed PHI, or to have been responsible for the incident;
- A description of where the PHI is believed to have been improperly transmitted, sent, or utilized, if applicable;
- A description of the probable causes of the incident;
- A description of the proposed plan for preventing similar future incidents, including ongoing risk remediation plan approval; and
- Whether the Practice believes any federal or state laws requiring notifications to individuals are triggered.

Incident Reporting (continued):

Reports must be sent to MLARA's Point of Contact:
Forrest Pasanski, Director

Enforcement Division

Bureau of Professional Licensing

PHONE: 517-242-6078

EMAIL: PasanskiF1@michigan.gov

611 West Ottawa

3rd Floor, Lansing, MI 48909

Mitigation by the Practice

The Practice and its Authorized Users shall mitigate, to the extent practicable, any harmful effect that is known to the Practice of a use or disclosure of PHI by the Practice in violation of the requirements of this Agreement, and report its mitigation activity back to MLARA. The Practice shall preserve evidence.