

November 5, 2015

Kelsey A.H. Maxim, PharmD  
981 Rook Way  
Sparks, NV 89441

Nevada State Board of Pharmacy  
431 W. Plumb Lane  
Reno, NV 89509

Dear Board Members,

I graduated from the University of Utah College of Pharmacy in May 2014 and have been a Nevada registered pharmacist since June 2014. I am currently practicing with Molina Healthcare. Molina Healthcare is a managed care company headquartered in Long Beach, California. For over 35 years, Molina has served members, partnered with providers, supported local communities and worked with state and federal governments. Molina Healthcare's mission is "to provide quality health services to financially vulnerable families and individuals covered by government programs". Molina has several types of health plans, including Medicaid, Medicare, integrated Medicaid/Medicare (Duals) and Marketplace plans. I specifically work within Molina's Medicare division, located in Midvale, Utah, performing medication therapy management services to our Part D members remotely.

I was recently informed that pursuant to NAC 639.403, "a registered pharmacist must apply to the Board to engage in the practice of pharmacy at a site other than the site of a licensed pharmacy by submitting an application on a form prescribed by the Board". I previously did not understand this statute and at this time would like to request not only the permission, but also the support of the Nevada State Board of Pharmacy in order to provide cognitive pharmaceutical services to Molina's Medicare Part D members from a location other than a dispensing pharmacy or healthcare facility.

The activity that I am requesting permission to perform is medication therapy management (MTM) pursuant to 42 C.F.R. § 423.153(d). The Molina Medicare Medication Therapy Management Program (MTMP) is a clinical pharmacy outreach service designed to educate patients and their health care team in order to optimize medication-related health care outcomes, ensure patient safety, recommend cost-effective medication strategies, coordinate care with the member's interdisciplinary care team and comply with Centers for Medicare and Medicaid Services (CMS) guidelines.

According to CMS, section 10328 of the Affordable Care Act amended section 1860D-4(c)(2)(ii) of the Act to "require prescription drug plan sponsors to offer, at a minimum, an annual comprehensive medication review (CMR) that may be furnished person-to-person or via telehealth technologies. A CMR is an interactive, person-to-person or telehealth medication review and consultation of a beneficiary's medications (including prescriptions, over-the-counter (OTC) medications, herbal therapies, and dietary supplements) by a pharmacist or qualified provider that is intended to aid in assessing medication therapy and optimizing patient outcomes. The CMR must include a review of the individual's medications, which may result in

the creation of a recommended medication action plan with a written or printed summary of the results of the review provided to the targeted individual.”

Molina Medicare Part D members can qualify for MTM services by fulfilling the following: three or more chronic diseases (i.e. asthma or COPD, chronic heart failure, diabetes mellitus, dyslipidemia, hypertension or mental health) and have six or more covered Part D chronic/maintenance drugs per month, or projected incurred cost of \$3,016 or more per year in covered Part D drugs as calculated by \$784 or more incurred cost in previous quarter.

Molina’s MTM services include analyzing a member’s medication list to review it for potential patient safety problems, drug interactions, suboptimal medication regimens, etc. We also work with the member to overcome barriers and poor adherence to medication therapy through motivational interviewing techniques, addressing financial concerns, transitioning the member from 30-day to 90-day supplies, providing pill boxes to improve adherence, or getting medications prior-authorized. Pharmacists also provide education to members and their health care providers about their medications, assist in coordination of care for pharmacy-related issues between members, providers and other members of the member’s interdisciplinary care team, and communicate identified suggested interventions to members’ providers.

Providing medication therapy management services is an exciting opportunity for pharmacists. Molina’s MTM program allows pharmacists the ability to act as a liaison between physicians and patients in order to help patients achieve the health results they need. I am excited about this opportunity that has arisen for our profession. I ask that the Board support my request to provide cognitive services from a non-pharmacy location and efforts to advance pharmacy practice through involvement in medication therapy management services.

Sincerely,

Kelsey A.H. Maxim, PharmD

**Application to apply to the Board to engage in the practice of pharmacy at a site other than the site of a licensed pharmacy**

1. The name of the pharmacist
  - a. *Kelsey A.H. Maxim, PharmD*
2. A description of the services that the pharmacist intends to provide at the site
  - a. *The Molina Medicare Medication Therapy Management Program (MTMP) is a clinical pharmacy outreach service designed to educate patients and their health care team in order to optimize medication-related health care outcomes, ensure patient safety, recommend cost-effective medication strategies, coordinate care with the member's interdisciplinary care team and comply with CMS guidelines.*
  - b. *Molina's MTM services include analyzing a member's medication list to review it for potential patient safety problems, including potential drug interactions, suboptimal medication regimens, etc. We also work with the member to overcome barriers to appropriate medication usage that may include analyzing resistance to adherence to therapy through motivational interviewing techniques, financial concerns, transitioning the member from 30-day to 90-day supplies, providing pill boxes to improve adherence, or to escort needed medications through the prior authorization process. Pharmacists also provide education to members and their health care providers about their medications, assist in coordination of care for pharmacy-related issues between members, providers and other members of the member's interdisciplinary care team, and communicate identified suggested interventions to members' providers.*
3. The location at which the pharmacist will provide the services
  - a. *Home office, located at 981 Rook Way Sparks, NV*
4. An identification of the types of patients or other persons to whom the pharmacist intends to provide the services
  - a. *Molina Medicare Part D members*
    - i. *Molina has Medicare Part D members in eleven states including California, Florida, Illinois, Michigan, New Mexico, Ohio, South Carolina, Texas, Utah, Washington, and Wisconsin*
    - ii. *Molina Medicare Part D members can qualify for MTM services by fulfilling the following: three or more chronic diseases (asthma or COPD, chronic heart failure, diabetes mellitus, dyslipidemia, hypertension or mental health) and have six or more covered Part D chronic/maintenance drugs per month, or projected incurred cost of \$3,016 or more per year in covered Part D drugs as calculated by \$754 or more incurred cost in previous quarter.*
5. An identification of the types of pharmacies or other entities to whom the pharmacist intends to provide the services
  - a. *See Section 4*
6. A description of all resources, both paper and electronic, that will be available to the pharmacist in the course of providing the services
  - a. *Recommendations will be based off current guidelines, including but not limited to the 2014 Eighth Joint National Committee's Guideline for the Management of High Blood Pressure in Adults (JNC 8), 2015 American Diabetes Association Standards of Medical Care in Diabetes, 2013 ACC/AHA Guideline on the Treatment of Blood Cholesterol to Reduce Atherosclerotic Cardiovascular Risk in*

- Adults, 2013 ACCF/AHA Heart Failure Guidelines, 2014 AHA/ACC/HRS Guideline for the Management of Patients with Atrial Fibrillation, 2013 ACCF/AHA Guideline for the Management of ST-Elevation Myocardial Infarction, 2014 AHA/ASA Guidelines for Prevention of Stroke in Patients with Stroke and Ischemic Attack, 2012 KDIGO Clinical Practice Guidelines for the Evaluation and Management of Chronic Kidney Disease, and the 2013 National Osteoporosis Foundation Clinician's Guide to Prevention and Treatment of Osteoporosis*
- b. *Online resources include Lexicomp, UpToDate, and Clinical Pharmacology*
  - c. *Textbook resources include Dipro's Pharmacotherapy Handbook 8<sup>th</sup> Edition, Koda-Kimble's Applied Therapeutics 9<sup>th</sup> Edition, and the Handbook of Nonprescription Drugs 17<sup>th</sup> edition.*
  - d. *Monthly CE's are also offered through Roseman University of Health Sciences to provide continuing education on chronic disease states that are often seen within our Medicare population*
7. The days and hours during which the pharmacist intends to provide the services
    - a. *Monday through Friday between the hours of 7:30am and 6:00pm and occasionally on a Saturday if requested by the member*
  8. An explanation of the policy of the pharmacist for users of the services when the pharmacist is unavailable
    - a. *Molina's MTMP department has a toll-free number that members can call in order to reach a pharmacist. The line is available from 7:00am to 5:00pm PST. Members can call this number, which is answered by a Molina representative, who then transfers the call to an available pharmacist (or the requested pharmacist) or schedules an appointment for the pharmacist to call the member back. This line also has a voicemail set up so members can leave messages if they call after office hours.*
  9. An explanation of the policy of the pharmacist regarding the confidentiality and security of the patient data that will be gathered, made and maintained as part of the services which are provided, including, without limitation, paper and electronic records
    - a. *Molina laptops have several security features including Check Point and a two-factor authentication system in order to log in to the VPN client.*
      - i. *Molina utilizes Check Point Software Technologies, which provides IT security, including Firewall, IPsec VPN, Mobile Access, Intrusion Prevention, Antivirus, Anti-spam and Email security, URL filtering, Data Loss Prevention, Anti-Bot and Application Control. Check Point provides these components as individual products called Software Blades or combined in one of their bundle offerings: Next Generation Firewall (NGFW), Next Generation Threat Prevention (NGTP), Next Generation Data Protection (NGDP) and Next Generation Secure Web Gateway (NGSWG)*
      - ii. *Two-Factor Authentication is a technology that provides identification of users by means of the combination of two different components. "These components may be something that the user knows, something that the user possesses or something that is inseparable from the user." Specifically, I use my username and password in combination with an application on my iPhone that provides me a number that must be entered within 30 seconds of being generated.*
      - iii. *In addition, please see attached, "Laptop Security Measures"*

- b. All printing is conducted in the office, located in Midvale, Utah. CMRs are completed using a third-party vendor called Assurance. Assurance is accessed through the Internet. Once a CMR is completed, it generates reports to be sent to both the member and the member's provider. Clerks in Midvale print and mail the patient reports and fax the provider reports to a verified-fax number.*
- 10. Whether the services provided will be affiliated with, an adjunct of or otherwise related to a licensed pharmacy
  - a. Not applicable*
- 11. A description of the business plan for the services provided
  - a. Please see attached, "Medication Therapy Management Program 2014 Detailed"*

## Medication Therapy Management Program Description:

The Molina Medicare Medication Therapy Management Program is a clinical pharmacy outreach service designed to educate patients and their health care team in order to optimize medication-related healthcare outcomes, ensure patient safety, recommend cost-effective medication strategies, coordinate care with the member's interdisciplinary care team and comply with CMS guidelines.

**Interventions:** the Medication Therapy Management Pharmacists:

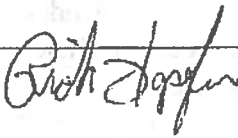
- Provide a *comprehensive medication review (CMR)* for all eligible members annually
  - Analyze member's medication lists
  - Review medication lists for potential patient safety problems, including potential drug interactions, suboptimal medication regimens, etc.
  - Make outbound calls to members and speak with them about their medications in an interactive person-to-person consultation
  - Work with the member to overcome barriers to appropriate medication usage:
    - Resistance to adherence to therapy through Motivational Interviewing techniques
    - Financial concerns:
      - Transition members from brand-name or non-formulary medications to more cost-effective or generic alternatives
      - Educate the member on how to optimize their medications to the formulary
      - Save copays by refilling medications only every 90 days instead of monthly
    - Enable the member to transition from 30-day to 90-day supplies for improved adherence.
      - Provide overrides in the pharmacy billing system so all 90-day supplies can be picked up at one time from the local pharmacy
      - Escort the member through the process of transferring medications to mail order through CVS/Caremark
    - Provide pill boxes to enable improved adherence.
      - Provide a chart which shows the best times for daily administration in order for the member to fill the pill box themselves.
    - Escort needed medications through the prior authorization process.
  - Provide education to members about their medications including:
    - the importance and benefits of the medications relevant to the members' medical conditions.
    - Potential side effects that the members may experience.
    - How to overcome side effects of medications
    - Helping member to weigh the risks and benefits of each therapy.
  - Provide education to members' health care providers about the members' medications
  - Assist in coordination of care for pharmacy-related issues between members, providers and other members of the member's interdisciplinary care team
  - Communicate identified suggested interventions to members' providers
  - Document interactions with members and providers
  - Send a reconciled personal medication list to members once comprehensive review is completed
- Conduct *targeted medication reviews* for eligible members quarterly
  - Follow-up with members to ensure changes are being made to meet treatment goals

- Target specific clinical problems that affect many members and send letters to prescribers

**Eligibility for MTMP:** members can qualify for the MTMP by fulfilling the following:

- Three or more of the following chronic diseases
  - Respiratory Disease-Asthma
  - Respiratory Disease-COPD
  - Chronic Heart Failure
  - Diabetes Mellitus
  - Dyslipidemia
  - Hypertension
  - Mental Health-Depression
  - Mental Health-Chronic and Disabling
- AND six or more covered Part D chronic/maintenance drugs per month
- Projected incurred cost of \$3,016 or more per year in covered Part D drugs as calculated by \$784 or more incurred cost in previous quarter

# MOLINA HEALTHCARE INC.

	<b>Policy and Procedure No.</b> IS-61.20
	<b>Department:</b> Information Services
	<b>Title:</b> Desktop/Laptop Security Standards
	<b>Effective Date:</b> September 3, 2013
	<b>Reviewed and Revised Date:</b> 11/19/13,12/24/14, 7/20/15
Rick Hopfer CIO	<b>Reviewed Only Date:</b>
<b>Authorized Signature:</b>  <b>Date:</b> 7/27/15	<b>Supersedes and replaces:</b> IS-61.20 <b>Date:</b> May 1, 2008

## I. PURPOSE

The purpose of this document is to provide guidance for Molina Healthcare, Inc. (MHI), regarding desktops and laptops to ensure the security of information.

Desktops or laptops provide access to MHI's data. If the desktop or laptop has weakness in security, it will be exploited. Therefore, it is important to have strong security standards for all desktops and laptops.

This document applies to all MHI workforce members, consultants, vendors, and guests, using a desktop or a laptop that is connected or will be connected to the MHI network.

## II. POLICY

Workforce members using laptops or desktops shall consider the sensitivity of the information, including electronic Protected Health Information, (e-PHI), including Race/Ethnicity and Language (REL) Data and other sensitive member information, that may be accessed; and shall minimize the possibility of unauthorized access.

MHI will implement physical and technical safeguards for all desktops and laptops that access ePHI or other sensitive member information shall be limited to minimum necessary required to perform their job related duties.

## III. PROCEDURE

Appropriate measures must be taken when using desktops or laptops to ensure confidentiality, integrity, and availability of sensitive information, including Protected Health Information (PHI) and that access to sensitive information is restricted to authorized users only.



Policy and Procedure No: IS-61.20	Department: Information Services
Title: Desktop/Laptop Security Standards	

Appropriate measures include:

- Users *must not* install, copy, or distribute any software on a desktop or laptop. This includes but is not limited to: Audio files, movies, photographs, games, books, hacking tools, third-party browsers, etc. Exceptions will be made if the software is required to perform their job function. All exceptions must be approved by either the Chief Information Security Official or his designee.
- Users must not have Administrator-level rights either for a desktop or laptop. Under special circumstances and upon the approval of either the Chief Information Security Official or his designee, the user can be provided with Local Administrator rights. Approved users for any use of administrator rights shall use the Privilege Account Manager (PAM) tool when accessing administrative accounts. All approvals shall be documented and approved by IT Security. This requirement will lessen security threats and vulnerabilities on desktops and laptops.
- All company laptop and desktop hard drives will be encrypted with certified FIPS 140-2 disk encryption software that will include pre-boot authentication where necessary. Devices identified out of compliance shall be removed from Active Directory (AD) by the FTS team and returned to the IT department immediately to be re-imaged to ensure compliance.
- All MHI desktop and laptop computers shall be configured according to MIT desktop and laptop configuration standards.
- Restrict physical access to laptops and desktops to only authorized personnel.
- Ensuring laptops are not left unattended in public places on or off MHI property.
- Securing laptops and desktops (screen lock or logout) prior to leaving area to prevent unauthorized access.
- Users issued laptops are expected to take them home at the end of the business day. In addition to working remote, this also provides for off-site business continuity in the event of a disruption of services.
- Keep food and drink away from laptops and desktops in order to avoid accidental spills.
- Secure laptops by using cable locks or locking up laptops in drawers or cabinets where necessary.
- View screens/monitors are positioned away from public view. If necessary, install privacy screen filters or other physical barriers to public viewing.
- If using a wireless network, ensure access is secure by following the Wireless Network Security policy.
- If network connectivity is required during hotel stays, the user should opt for a wired connection if one is available.
- When transported by car, laptops should be stowed in the trunk or some other area where it will not be easily seen or attract attention.
- When traveling by air or train, the laptop should never become checked baggage and should always be kept as carry-on luggage. During hotel stays, laptops should not be left unsecured in the room. If the user cannot take the laptop with them when leaving the hotel, it should be secured with a cable lock or left in the hotel safe.
- Users shall not disable any default software applications, such as antivirus software, encryption software, and desktop agents (desktop management service) deployed by the MIT Enterprise Service Desk.

- Desktop and laptop computer users shall not write, compile, copy, knowingly propagate, execute, or attempt to introduce any malicious computer codes designed to self-replicate, damage, or otherwise hinder the performance of any computer system, such as a virus, worm, or Trojan horse.
- Unauthorized or non-MHI-provided desktops or laptops are not allowed to connect to the MHI network to access data or any resources. The ONLY exceptions to this rule are for users who access through Citrix SSL VPN with two-factor authentication..
- All remote connections to Molina’s Web Mail (OWA), Molina’s network using the VPN Client, and to Molina’s applications using the Citrix SSL VPN shall utilize two-factor authentication provided by MHI Information Technology (IT) Department.
- Suspected viruses or security incidents should be reported immediately to the CIRT.
- User accounts that are associated with potential security incidents may be disabled or have the password reset by the Computer Incident Response Team (CIRT) until an investigation is completed to ensure compliance.
- Lost or stolen workstations or laptops must be reported immediately to the Security Officer or the Privacy Officer.

**IT Security Standard(s)**

Please refer to the following standard(s) for procedural specific requirements that must be followed by IT staff: IS 61.20 Desktop and Laptop Standard

**IV. DEFINITIONS**

- *Workforce* includes employees, agency labor, volunteers, trainees, and other persons whose conduct, in the performance of work for MHI is under the direct control of MHI.
- A *workstation* is a hardware device used for MHI business and includes desktop computers, laptop computers, Personal Digital Assistant (PDA), or other devices that perform similar functions,
- *Protected Health Information (PHI)* means Individually Identifiable Health Information, except as noted below, that is:
  - a. Transmitted by electronic media;
  - b. Maintained in electronic media; or
  - c. Transmitted or maintained in any other form or medium.

Protected Health Information excludes Individually Identifiable Health Information:

- (i) in educational records covered by the Family Educational Rights Privacy Act;
- (ii) in records described at 20 U.S.C. 1232g(a)(4)(B)(iv);
- (iii) in employment records held by Molina Healthcare in its role as an employer; and
- (iv) regarding a person who has been deceased for more than 50 years.

- *Sensitive Member Information* means PHI and other Individually Identifiable Health Information that Molina Healthcare members would reasonably want to keep private and confidential.
- *Individually Identifiable Health Information* is information that is a subset of health information, including demographic information (which includes, but is not limited to, Race/Ethnicity and Language Data) collected from an individual, and
  1. Is created or received by health care provider, health plan, or health care clearinghouse; and
  2. Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and
    - (i) that identifies the individual; or
    - (ii) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.
- *Confidential Information* includes, but is not limited to, protected health information (PHI), personal information concerning members, employees and providers; practitioner specific information related to credentialing proceedings, quality reviews, malpractice suit, peer-reviewed determination etc.; financial information relating to members, employees and providers; proprietary business information and trade secrets.
- *Electronic Confidential Information* includes confidential information stored or transmitted electronically.
- *Encryption* is the conversion of data into a form, called a ciphertext that cannot be easily understood by unauthorized people. Decryption is the process of converting encrypted data back into its original form, so it can be understood.
- A *laptop (notebook) computer* is a portable computer. Laptop computers allow the user to bring the computer with them, and the main risks of such a computer are having the computer stolen and logging onto an unsecure network whereby compromising the security of the data on the computer.
- *Administrator-level rights* are the highest level of permission that is granted to a computer user and normally allows the user to install software, and change configuration settings
- A cable lock is an anti-theft system designed to secure a laptop to a permanent surface. The lock attaches to a small, metal-reinforced hole found commonly on small or portable computers and electronics equipment
- *Wi-Fi* is a technology that allows an electronic device to exchange data or connect to the Internet wirelessly, using radio waves. It connects via a wireless local area network (WLAN) through the use of a wireless router.
- A *server* is a dedicated computer or device on a network that manages network resources, such as documents, sound files, photographs, movies, images, and databases.
- *Malicious computer code (malware)* is software used—and sometimes programmed—by attackers to disrupt computer operation, gather sensitive information, or gain access to a computer. Malware

includes computer viruses, ransomware, worms, Trojan horses, rootkits, keyloggers, dialers, spyware, and adware.

- *Citrix SSL VPN* (virtual private network) extends a private network securely encrypting traffic across a public network, such as the Internet. It enables a computer to send and receive data across shared or public networks as if it were directly connected to the private network, while benefiting from the functionality, security and management policies of the private network.
- *Two-factor authentication* requires the presentation of two or more of the three *independent* authentication factors: a *knowledge* factor ("something only the user *knows*"), a *possession* factor ("something only the user *has*"), and an *inherence* factor ("something only the user *is*"). After presentation, each factor must be validated by the other party for a successful authentication to occur.