DEPARTMENT OF THE NAVY
BUREAU OF MEDICINE AND SURGERY
7700 ARLINGTON BOULEVARD
FALLS CHURCH VA 22042

IN REPLY REFER TO
BUMEDINST 6300.22
BUMED-M3
7 Jun 2018

BUMED INSTRUCTION 6300.22

From: Chief, Bureau of Medicine and Surgery

Subj: SECURE MESSAGING SERVICE

Ref: (a) DoD 6025.18-R, Department of Defense Health Information Privacy Regulation, January 2003
(b) DoD Instruction 8580.02 of 12 August 2015
(c) BUMEDINST 6000.16
(d) BUMEDINST 6300.19
(e) OPNAVINST 6400.1C
(f) BUMEDINST 5211.4

Encl: (1) Secure Messaging Business Rules

1. Purpose. Provide guidance on the implementation, utilization, and sustainment of secure messaging by Navy Medicine (NAVMED) clinicians and staff as the preferred means of privacy-compliant electronic communication with patients.

2. Scope and Applicability. This instruction applies to all primary and specialty care services, as well as clinical outpatient and administrative services equipped with secure messaging capabilities. Detailed instructions on how to perform the tasks directed in this policy can be found in enclosure (1).

3. Background. Secure messaging is a service provided by a contract vendor that allows patients, staff, and clinicians to asynchronously communicate about non-urgent issues on a platform that conforms to privacy and informatics requirements. Secure messaging is aligned with the quadruple aim and 2014 Military Health System (MHS) review findings, available at http://www.health.mil/Military-Health-Topics/Access-Cost-Quality-and-Safety/MHS-Review. It provides patients with virtual care options, is a significant patient satisfier, and is an efficient care coordination and population health management tool for Medical Home Port (MHP) teams. Secure messaging service is also a requirement of all third party patient-centered medical home accrediting organizations and a necessity for NAVMED and the MHS to remain relevant in an age of rapidly advancing technology. In coordination with Defense Health Agency (DHA) Solutions Delivery Division, the Bureau of Medicine and Surgery (BUMED), Healthcare Operations (BUMED-M3) deployed secure messaging capabilities to all primary care clinics, and will continue to deploy capabilities across specialty care as opportunities are identified. Standardized business rules, metrics, guidance on enrollment use, best practices, and oversight will maximize the benefit of the service.

4. Policy. All clinics equipped with secure messaging capabilities must implement, measure, and enforce the utilization of secure messaging as the preferred Health Insurance Portability and Accountability Act (HIPAA) of 1996 compliant form of electronic communication. Under no circumstances should regular e-mail be used as a communication tool for patient care. Per references (a) through (c), all current local, State, and Department of Defense (DoD) regulations identifying eligibility for care, consent for care, parental notifications, emancipation guidelines, power of attorney guidelines, and HIPAA guidelines apply.

5. Action. Full compliance with the provisions of this instruction is expected for all commanding officers (CO) and officers in charge (OIC) of facilities implementing and sustaining a secure messaging program. Oversight and assistance with implementation and sustainment of performance must be provided by NAVMED East and NAVMED West in collaboration with BUMED-M3. BUMED-M3 maintains and updates resources for implementation and monitoring available at https://community.max.gov/display/ DoD/ Secure+ Messaging+Home. All clinics equipped with secure messaging capabilities must implement, measure, and enforce the utilization of secure messaging per policies outlined in paragraph 4 of this instruction and reference (d).

6. Responsibilities

a. Assistant Deputy Chief, (BUMED-M3) must:

(1) Provide strategic guidance and direct oversight of the implementation and execution of secure messaging.

(2) Coordinate with the DHA, BUMED-M3, Tri-Service governance boards, and NAVMED regions as appropriate to pursue standardization in strategy and revise key metrics and targets.

(3) Provide secure messaging data dashboard on a monthly basis via the max.gov Web site https://community.max.gov/display/ DoD/ Secure+ Messaging+Home or other accessible platform.

(4) Support medical treatment facilities (MTF) and clinics in the deployment and sustainment of this service based on strategic needs.

(5) Facilitate monthly informational calls.

(6) Coordinate with the vendor, NAVMED regions, and MTFs to identify and support training needs for clinic staff.

(7) Actively communicate and promote the use of the service to the NAVMED regions, MTF leadership, and relevant stakeholders.

b. Commanders, NAVMED Regions must:

(1) Appoint in writing a regional secure messaging champion responsible for providing support necessary to ensure all subordinate MTFs implement and comply with the direction set forth in this instruction.

(2) Enforce compliance and promote a culture of continuous performance improvement around the efficient utilization of the service as well as the metrics and associated monitoring processes.

(3) Review the data dashboard monthly and follow up on performance outliers.

(4) Attend monthly calls and facilitate sharing of best practices across MTFs within their area of responsibility.

(5) Actively engage subordinate commands to identify clinics that are not yet equipped with secure messaging and facilitate communication with the vendor via BUMED-M3 to deploy licenses and training as appropriate.

c. MTF COs and OICs must:

(1) Maintain compliance and promote a culture of continuous performance improvement around the efficient utilization of the service as well as the metrics and associated monitoring process set forth in this instruction.

(2) Actively communicate and promote the use of secure messaging and its benefits to clinicians, staff, and eligible beneficiaries.

(3) Work with directorates and departments to ensure all primary care clinicians and clinic staff are connected.

(4) Identify additional clinics that are ready to leverage and incorporate secure messaging capabilities into their workflow. In the interest of responsible stewardship of the finite number of available licenses, connection of clinics that do not have the need for the service or are not prepared to adopt it into their workflow is discouraged.

(5) Appoint in writing and maintain one or more secure messaging champion(s) for the command. While not required, it is recommended to designate clinic and branch clinic level champions. Secure messaging champions should be afforded sufficient administrative time away from patient care responsibilities to fulfill the duties of the position. Ensure the champion(s) execute the responsibilities designated in paragraph 6d of this instruction and enclosure (1).

d. MTF Secure Messaging Champions, Super Users, and Administrators must:

(1) Ensure each clinic with secure messaging capabilities has at least one secure messaging administrator and that the administrator receives appropriate training on configuration and maintenance of accounts for staff and patients.

(2) Analyze the data dashboard monthly, work with clinics to improve metric outliers, and communicate performance to MTF leadership and necessary stakeholders at least quarterly.

(3) Work with MTF leadership, privacy representatives, and chief informatics officers to integrate secure messaging workflows into command policy and regulation, and ensure adequate technical support.

(4) Work with directorates and departments to ensure all primary care clinicians and clinic staff are connected, and identify additional clinics that are ready to leverage and incorporate secure messaging capabilities into their workflow. Submit requests to connect new clinics to BUMED-M3 shared mailbox (usn.ncr.bumedfchva.mbx.bumed-mhp-pmo@mail.mil) and support newly connected clinics in establishing and maintaining successful workflows.

(5) Attend monthly calls, and disseminate policy, metric targets, and best practices to clinics; assist clinics to implement best practices.

(6) Communicate with all connected clinics about vendor-hosted virtual trainings and request and coordinate on-site training via NAVMED regions and BUMED-M3 if needed.

(7) Conduct regular account maintenance and oversee the effort to add and remove clinicians and staff as part of the MTF check-in and check-out processing.

(8) Troubleshoot problems and escalate concerns to the NAVMED regional champion, BUMED-M3, or the vendor customer support as appropriate.

7. Metrics Monitoring. In order to track performance and identify outliers, share best practices across NAVMED and the MHS, and proactively identify and resolve systemic issues, BUMED-M3 follows key metrics as determined by NAVMED and MHS governance bodies. The metrics in subparagraphs 7a and 7b of this instruction are currently monitored, though measures and current targets may be subject to change in the future. MTFs are expected to meet and maintain performance consistent with the "green" target on any secure messaging metric identified as a priority across the MHS.

a. Secure Messaging Connections. The percent of all enrolled patients who have accounts.

b. Clinic Response Time. The percent of new incoming messages responded to within 8 business hours.

8. Etiquette. Correspondence from MTF staff via secure messaging is equivalent to any other form of communication with beneficiaries, and as such, must be at all times professional and courteous. Beneficiaries must be addressed by appropriate rank or title as they would normally be in person or on the phone. Care must be taken by all staff to ensure patient privacy is respected and that information is not inadvertently sent to the wrong patient.

9. Utilization by Privileged and Non-Privileged Providers. Utilization of the service by clinicians must abide by the same oversight and guidelines as the provision of virtual care via telephone consults. Providers who require supervision in the completion of other virtual patient care activities must abide by the same guidelines in their use of secure messaging. Independent Duty Corpsmen must adhere to guidelines set forth in reference (e).

10. Transition to MHS GENESIS. As MTFs transition to the new electronic health record (EHR), the patient portal platform, logistics of monitoring and responding to message traffic, and collection of data for secure messaging performance metrics may change. However, commands and clinics are expected to follow the same business rules outlined in enclosure (1) in the management of the overall secure messaging program and in responding to patient needs.

11. HIPAA Breach Reporting

a. The secure messaging system provided by the company previously known as RelayHealth, now Change Healthcare Engagement Solutions, allows an individual to manage the account of another individual, such as a child, spouse, or parent, and interact with the clinic on that person's behalf. In situations where an individual is managing the account of another adult, age 18 or older, the clinic must verify legal documentation authorizing the primary account holder to access the other individual's health information, such as a DD Form 2870 Authorization for Disclosure of Medical or Dental Information, medical power of attorney, court order of guardianship, or other qualifying documentation.

b. In the event of a HIPAA violation or privacy breach occurring in subparagraph 11a of this instruction or any other scenario, MTF staff must immediately contact the MTF champion and the vendor to extract the erroneous message, and report the incident per references (a), (b), and (f).

c. Under Government reporting requirements, the breach must be reported within 1 hour of discovery to the MTF privacy officer, BUMED privacy officer, and within 24 hours of discovery to the DHA privacy office and Department of the Navy Chief Information Officer using SECNAV 5211/1 Department of the Navy (DON) Loss or Compromise of Personally Identifiable Information Breach Reporting Form. The Agency is deemed to have discovered a breach as of the time a breach (suspected or confirmed) is known or by exercising reasonable diligence, or would have been known to any person (other than the person committing it) who is an employee, officer, or other agent of the agency.

d. Breaches must be reported to BUMED-M31 at USN.ncr.bumedfchva.list.bumed-pii-rpt@mail.mil.

12. Review and Effective Date. Per OPNAVINST 5215.17A, BUMED-M3 must review this instruction annually on the anniversary of its effective date to ensure applicability, currency, and consistency with Federal, DoD, Secretary of the Navy, and Navy policy and statutory authority using OPNAV 5215/40 Review of Instruction.

13. Records Management. Records created as a result of this instruction, regardless of media and format, must be managed per Secretary of the Navy Manual 5210.1 of January 2012.

14. Forms and Information Management Control

a. Form. DD Form 2870 Authorization for Disclosure of Medical or Dental Information is available at http://www.dtic.mil/whs/directives/forms/eforms/dd2870.pdf.

b. Information Management Control. The reports required in subparagraphs 6a(3) and 11a through 11d of this instruction are covered in references (a), (b), and (f).

TERRY J. MOULTON
Acting

Releasability and distribution:
This instruction is cleared for public release and is available electronically only via the Navy Medicine Web site, http://www.med.navy.mil/directives/Pages/BUMEDInstructions.aspx.

BUMEDINST 6300.22
7 Jun 2018

SECURE MESSAGING BUSINESS RULES

1. Overview. As the usage of secure messaging increases across the enterprise, business rules to guide enrollment, use, maintenance, and oversight are necessary to ensure standardization of the service. These business rules are meant to provide the "rules of the road" for effectively utilizing secure messaging and maximizing its impact.

2. Refrain from Use of Brand Name. The vendor may change over time. Change Healthcare Engagement Solutions is the current vendor. The vendor's title must only be used when referring to representatives currently contracted to deliver secure messaging to the Navy, or to specific functions of the vendor's platform. The vendor provides training and core functions; however, the patient portal for secure messaging is distinct from the vendor. To avoid use of brand names, standard internal communications must refer to the patient portal for secure messaging or TRICARE online patient portal for secure messaging.

3. Staff and Provider Accounts and Maintenance

a. Secure Messaging Accounts. All primary care staff members must have secure messaging accounts. Connecting and disconnecting staff must be part of the check-in and check-out process within each department and the command. When members move to a new MTF, accounts must be disconnected at the previous clinic in order for the new clinic to connect them. Additionally, patient connections must be removed from providers before their accounts can be disconnected from a clinic. Staff who have left the Navy must not have continued access to DoD patient records via secure messaging, and these accounts must be turned off entirely.

(1) Adding or Deleting Providers: While super users are able to add or delete accounts for other staff, provider connections must always be managed through the vendor's customer support. Requests for provider "adds" and "deletes," as well as any other requests for technical support must be submitted through the customer support desk by e-mail. If requests are submitted before 1 October 2018 use t1support@relayhealth.com; or is submitted after 1 October 2018 use FederalProviderPortal Support @Changehealthcare.com. Customer support can also be reached by telephone at (866) 735-2963 (option 1).

(2) Provider connection requests sent to customer support must include the legal name of the provider, name of the practice and team, and name of the provider being replaced if relevant, such that customer support may move the patient panel from the outgoing to incoming provider.

(a) Before 1 October 2018, to connect a new provider without a previously existing account, the provider must first create an account at https://mil.relayhealth.com before the request is submitted to customer support. After 1 October 2018, new providers must create their accounts at www.TOLSecureMessaging.com.

(b) To disconnect a provider, all patient connections must be moved to another provider before the request is submitted to customer support.

(c) Removal of patient connections and disconnection of an outgoing provider is essential in order for that provider to be gained at the next MTF.

b. Secure Messaging Account Maintenance. Each clinic must designate a super user to perform account maintenance checks every month to ensure staff and patients who have left the command are appropriately disconnected. To prepare the system for updates, some clinics have found it helpful to work with health benefits as a means of obtaining information from patients about their new assignments.

3. Secure Messaging Response Time Requirement. Responding to secure messages in a timely manner is critical to fulfilling the promise of high quality and accessible health care. With this in mind, all secure messages must be responded to within 8 business hours. Subparagraphs 3a through 3d of this enclosure provide the answers to some frequently asked questions:

a. What Counts as a Response. Any response to a patient within 8 business hours will satisfy the response time requirement. Business hours are defined by the vendor as Monday-Friday 0900-1700 in the time zone of the provider receiving the message, excluding major holidays. The response time applies only to the first message sent by the patient on a message thread. When the clinic messages back and forth with a patient on the same string, subsequent "replies" by the patient on the same message string do not generate a response time expectation.

b. Who Responds to Messages. All clinic staff are able to answer the vast majority of secure messages and their responses will help commands meet the response time requirement. Clinics' use of secure messaging must mirror the team-based practice used in other clinic activities, meaning all staff must be responsible for responding to messages appropriate for their training and role.

c. How Response Time is Measured. Response time measures how much time passes before a response is provided to an incoming message.

d. Response versus Resolution. Clinics must strive to fully resolve patients' requests within 8 business hours to the greatest extent possible. Generic responses used only to satisfy the response time requirement may be leveraged only when necessary for more complex requests that require additional time, but must not be used as a standard business practice for every message response.

4. Secure Messaging New Practice Upload Requests. When a command needs to bring a new clinic online that previously has not had secure messaging services, a new practice upload request must be submitted by the command's secure messaging champion to BUMED-M3. BUMED-M3 will obtain approval from DHA Solutions Delivery Division. Once approved,

BUMED-M3 will coordinate with the command secure messaging champion and the clinic to determine the best configuration for the practice, and provide a practice upload spreadsheet to fill in with practice, staff, and provider information.

5. Connecting Patients

a. Secure Messaging Patient Connection Verification. When a patient is sent the link to set up an account, he or she must then send a request to communicate with his or her provider(s) online. Patients may also set up their own accounts and then may request to connect to a provider(s). Should a patient request be declined, staff must provide the patient with a reason and redirect as appropriate. Clinic staff or providers may approve or decline a patient's request based on the following considerations:

(1) Patient name, gender, date of birth, etc., matches existing clinic records.

(2) Requestor is a current patient of the practice.

(3) Clinics may determine internally if patients should be allowed to connect only to the provider to whom they are empaneled, or to other providers in the practice they may have seen.

b. Prohibition of the Use of Physical Sign-Up Forms

(1) Secure messaging sign-up forms that are produced by the MTF to create a secure messaging account for a patient beneficiary (e.g., MTF personnel creating a patient account on behalf of the beneficiary) are not authorized.

(2) This process poses a security risk. The current vendor's system does not include a feature that forces users to change the password upon log in after the account is created; thus, the initial password remains indefinitely until it is changed by the patient. Many patients will never change the password provided to them by clinic staff, leaving their account accessible to others.

(3) When the account is created, the user (patient) must "accept" the vendor's terms of use and privacy agreements. The terms of use is a binding contract and informs the patient of their rights and responsibilities, as well as the rights and responsibilities of the vendor. The terms of use also contain an indemnification clause. Creating the account for the patient does not give them the opportunity to decline the terms of use or refuse the account should they have concerns about the vendor's use of their data.

c. Multiple User Accounts. To the extent that they remain HIPAA compliant, family accounts are allowed when beneficiaries prefer to have a family member send and receive messages on their behalf. Individual accounts are strongly encouraged as the preferred configuration when logistically feasible for the patients.

(1) Adolescent Accounts. Adolescents 13 years and older are able to establish individual accounts, such that they may message with their care team independently without parental access to their messages. State laws may govern local processes regarding the privacy of adolescents and age at which such rights take effect. MTFs must abide by local laws if different from those of the vendor. State laws also apply regarding minors' mental capacity and legal right to consent independently to proposed medical recommendations.

(2) Minors Under Age 13. Minors under the age of 13 may only be signed up for secure messaging via an adult surrogate. Additionally, surrogates may be established for adults who are incapable of managing their own health affairs or who do not have access to or prefer not to personally use the technology. In either case, verification of legal guardianship, medical power of attorney, and written authorization must follow the same laws and guidelines that apply when communicating with an adult surrogate about another's health in person or by telephone. In the case of surrogacy being assigned for a consenting adult, the DD Form 2870 must be used to document authorization.

(3) Adults Age 18 and Older. When adults aged 18 or over desire or require their account to be managed by another individual, clinics must verify and keep on file appropriate documentation legally authorizing the adult dependent relationship, such DD Form 2870, medical power of attorney, court order of guardianship, or other qualifying documentation. Adult patients whose accounts are to be legally managed by another individual must be added to the dependent exclusion list within the system.

(4) Automatically Separate Accounts. Clinics must enable the automatic separation configuration that notifies primary account holders of the need to disassociate or exclude child dependents as they approach age 18 and automatically disables accounts once the child turns 18 years old. The accounts can be reactivated either by the clinic obtaining legal documentation for the continued relationship and adding the patient whose account is being managed by another individual to the dependent exclusion list or by the primary account holder disassociating the account from his or her own.

d. Patient Permanent Change of Station (PCS) and Provider Changes. When a patient and his or her family execute a PCS move, there are three ways to ensure their secure messaging accounts are transferred to a new provider:

(1) The receiving MTF must offer registration to new patients who have not used secure messaging upon their check-in or invite a registered patient to connect to the new provider. The patient may also request connection to the new provider. BUMED-M3 recommends that all commands incorporate this into their check-in process for new patients.

(2) The losing command can disconnect the patient from their prior provider or the patient may disconnect themselves from the prior provider.

(3) When a patient is empaneled to a new provider within an MTF (such as when the previous provider PCS), it is the MTF's responsibility to transfer patients to the new provider in secure messaging.

6. Breach or Unintended Personal Identifiable Information (PII) or Protected Health Information (PHI) Disclosure Protocols

a. If a breach or unintended disclosure of PII or PHI occurs while using secure messaging, take the following measures:

(1) If a message containing PII or PHI is sent to an incorrect recipient, immediately notify the vendor's customer support at (866) 735-2963. The vendor will attempt to remove the message from the incorrect recipient's account before it is accessed. Customer support will be able to confirm if the message was successfully removed before it was incorrectly accessed.

(2) Report the situation to your privacy official or HIPAA security officer immediately, providing him or her with the vendor support ticket number.

b. For other cases of unintended disclosure, or if you suspect any kind of breach, contact your privacy official or HIPAA security officer immediately. Your privacy official or HIPAA security officer will take the necessary steps to comply with DoD privacy protocols and take appropriate action.

7. Workflow Considerations. MTFs and clinics must establish internal business rules regarding when and by whom messages are checked during each business day; how messages are distributed for action; and accountability for message resolution and metrics monitoring.

a. BUMED recommends utilization of dual computer monitors at each workstation, which increases efficiency of referencing patient information on multiple applications at once and transfer of messages into the EHR.

b. Clinics may determine which non-clinical message types do or do not need to be transferred into the EHR, such as requests for appointments or administrative assistance with booking a referral. Messages involving any clinical decision making or change to a treatment plan must always be documented in the EHR.

c. Clinic workflows must account for team member and provider absences. Responsibility and accountability for monitoring and responding to secure messages fall under the same business rules for checking lab and radiology results and telephone consult surrogacy. Setting an out of office on a provider's secure messaging account does not remove responsibility for responding to messages that are sent to that account.

d. Local business rules will govern how appointment requests should be addressed, to include working with the patient via messaging to set and book an appointment time and date or

contacting the patient by phone to more quickly facilitate the search for an agreeable appointment time. When the appointment request is handled by phone, a secure message response must still be sent to the patient afterward, both to meet the response time requirement and to provide the patient written confirmation of their appointment date and time.

8. Coding Guidance and Documentation

a. Coding Guide. The official MHS Coding Guidelines is available at https://info.health.mil/bus/brm/mcpo/SitePages/Home.aspx.

b. Documentation. All patient-to-provider communication that entails the provision of medical advice or that changes or otherwise affects the patient's care plan must be documented within the patient's medical record. The telephone consult module may be used to document both telephone and electronic communications.

c. Communication Between Patient and Provider. Documentation guidelines for electronic communication between patient and provider or the care team include a demonstration of the team's timely response to the patient's inquiry and involve the permanent storage of this communication. Documentation includes the sum of communication including related telephone calls, prescription refills, or laboratory orders associated with the same online encounter.

d. Privileged and Non-Privileged Providers. When supervision in the provision of virtual care is required by licensing and credentialing guidelines or by instruction, documentation must include the name of the supervising provider, and the supervising provider must sign or co-sign the encounter.

e. Privileged Provider Codes. The following are privileged provider codes to ensure standardization through the MHS is provided:

(1) 99441: Telephone evaluation and management service provided by a privileged provider to an established patient, parent, or guardian not originating from a related evaluation and management service provided within the previous 7 days nor leading to an evaluation and management service or procedure within the next 24 hours or soonest available appointment; 5-10 minutes of medical discussion.

(2) 99442: 11-20 minutes of medical discussion.

(3) 99443: 21-30 minutes of medical discussion.

(4) 99444: Online evaluation and management provided by a privileged provider to an established patient, guardian, or healthcare provider not originating from a related evaluation and management service provided within the previous 7 days, using the internet or similar electronic communications network.

f. Non-Privileged Providers Codes. For nurses, corpsmen, and medical assistants to use the following codes, communications via telephone or electronic media must be initiated by an established patient.

(1) 98966: Telephone assessment and management service provided by a non-privileged provider to an established patient, parent, or guardian not originating from a related assessment.

(2) 98967: 11-20 minutes of medical discussion.

(3) 98968: 21-30 minutes of medical discussion.

(4) 98969: Online assessment and management provided by a non-privileged provider to an established patient, guardian, or healthcare provider not originating from a related assessment and management services provided within the previous 7 days, using the internet or similar electronic communications network.

g. Patient-Initiated Communications. Patient-initiated situations applicable for telephone and electronic communications include the following:

(1) A patient describes new symptoms and requests intervention or advice from the privileged provider.

(2) In response to a patient communication, a privileged provider makes a new diagnosis and prescribes new treatment.

(a) A patient describes ongoing symptoms from a recent acute problem or chronic health problem and requests intervention or advice from the privileged provider to treat ongoing acute problem or chronic health problem.

(b) In response to a patient communication, a privileged provider gives substantive medical advice, revises a treatment plan, prescribes or revises medication, recommends additional testing, or provides self-care or patient education information for new or chronic health problem.

(c) A patient requests interpretation of lab or test results with evidence that the privileged provider is giving substantive explanation and possibly making recommendations to modify treatment plan, revise medications, etc.

(d) In response to a patient communication, a privileged provider gives extended personal patient counseling that changes the course of treatment and affects the potential health outcomes.

h. Patient-Initiated Communications Not Previously Captured. There may be patient-initiated communications that do not meet the criteria listed in subparagraphs 8e through 8g of this enclosure which must be coded with a 99499. Administrative telephone calls or encounters of care that would not have previously been captured or coded will be captured as non-count and coded with 99499 in the evaluation and management and appropriate V Code as a diagnosis.

i. Provider Initiated Communication. Provider-initiated calls and messages must also be coded with 99499 as the evaluation and management code with the relevant diagnosis code.

j. Examples of Non-Count. The following list gives examples where telephone and electronic communications codes must be "non-count" (applies to privileged and non-privileged providers):

(1) Telephone or electronic services referring to an evaluation and management service performed and reported by the same provider, occurring within the past 7 days.

(2) Telephone or electronic services ending with a decision to see the patient within 24 hours or next available urgent visit appointment.

(3) Telephone or electronic services occurring within the postoperative period of the previously completed procedure.

(4) Provider-to-provider interaction (colleague-to-colleague messaging).

(5) Leaving messages on answering machines.

(6) Scheduling, billing, and administrative issues.

(7) Communication of non-clinical information.

(8) Telephone services completed by interns (post graduate year 1).

(9) Providing test results without any medical decision making.