



DAVID MAXWELL-JOLLY
Director

State of California—Health and Human Services Agency
Department of Health Care Services



ARNOLD SCHWARZENEGGER
Governor

DATE: September 29, 2009

MMCD All-Plan Letter 09-014

TO: ALL MEDI-CAL MANAGED CARE HEALTH PLANS

SUBJECT: EXHIBIT G, HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)

The purpose of this All Plan Letter is to provide clarification for the requirements included in Exhibit G, Health Insurance Portability and Accountability Act (HIPAA) currently in all managed care health plan contracts. This letter provides a summary of discussions from meetings the Department of Health Care Services (DHCS) held with representatives from the managed care plans. This letter is broken into three sections, Questions and Answers, Future Updates and Contract Sections Already Removed.

QUESTIONS AND ANSWERS

Question 1: Provision 1(A) defines Protected Health Information (PHI); however the definition of DHCS data is not clear. Does DHCS data include PHI, or is it synonymous with PHI?

Answer: DHCS data includes all information provided by DHCS, whether it is in an electronic, paper or oral form. PHI is protected health information and is defined as: individually identifiable health information that is transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium. Since some of the data from DHCS will not be PHI, data that is DHCS PHI is a subset of DHCS data.

Question 2: Provision 1(B) only addresses privacy and security "created or received on behalf of DHCS pursuant to this contract." This statement does not include "The Contracted Entity, its employees, agents and subcontractors." Previously, DHCS had asked the plans to insert similar language in some of our Privacy policies and procedures dealing with disclosures of member PHI. Yet this language only speaks to protecting PHI created or received on behalf of DHCS. Is that accurate? Additionally, the HIPAA Security regulations specifically cover electronic PHI that is "created, received, maintained, or transmitted." Maintenance and transmission is not covered in this contract amendment language; however in the plans' current contract, the security regulations and all applicable laws are covered.

Answer: DHCS agrees that the words "maintained or transmitted" should be added. This paragraph should state, "DHCS desires to protect the privacy and provide for the security of PHI disclosed, created, received, maintained or transmitted on behalf of DHCS pursuant to this Contract." The language, "The Contracted Entity, its employees, agents and subcontractors" can be added but is not necessary as the restrictions and conditions imposed on the Contractor by this contract will extend to any agents or subcontractors of the Contractor pursuant to paragraph D on page 6. This paragraph is included in the section on "Responsibilities of the Contractor" and requires the Contractor:

"To ensure that any agents, including subcontractors but excluding providers of treatment services, to whom Contractor provides PHI received from or created or received by Contractor on behalf of DHCS, agree to the same restrictions and conditions that apply to contractor . . ."

Question 3: For Provision 2(C), plans request examples of entities outside the treatment network that DHCS has in mind as being recipients of beneficiary lists. If none is named, the provision can be deleted as not applicable to plans.

Answer: This term requires the Contractor to provide DHCS with a list of all entities that are not part of its treatment network and to whom the Contractor gives names and addresses of Medi-Cal members. The list is only for entities that are not part of the Contractor's treatment network and, pursuant to this term, the list must be provided to DHCS within 30 calendar days of the execution of the contract and annually thereafter.

Question 4: In regards to Provision 3(C)(3), Plans already conduct background checks and annual HIPAA trainings. Are there specific background lists DHCS wants checked? It does not seem necessary to have these provisions in contract. HIPAA does not specify a confidentiality statement. It would be sufficient for the contract to require the contractor to implement policies and procedures for granting employees access to PHI.

Answer: DHCS does not require that specific background lists be checked, only that a background check be done. DHCS does require that all of the actions listed in 3(C)(3) be done, including execution of confidentiality statements. Even though HIPAA may not contain these specific requirements, as a covered entity, DHCS is required to adopt administrative, technical and physical safeguards to protect PHI. See 45 CFR 164.530(c). The actions listed in 3(C)(3) are among the safeguards that DHCS has determined are necessary for it to meet this obligation.

Question 5: Is Provision 3(C)(3)(a) intended to be a separate confidentiality statement in addition to the confidentiality statement signed by all new employees of a particular contracted entity as part of their terms and conditions for employment with the organization? Is there a Model Confidentiality Statement template DHCS can provide? Are all existing employees handling PHI expected to sign another confidentiality statement? This is not a federal requirement.

September 29, 2009

Answer: This Provision is not intended to impose the requirement of obtaining a second confidentiality statement in addition to a confidentiality statement already required of employees. It is intended to impose the requirement that all employees who have access to DHCS PHI sign a confidentiality statement before access is granted. If the confidentiality statement required of new employees meets the requirements set out in paragraph (3)(a), and is renewed annually, it will fulfill this requirement. If existing employees have not already signed a confidentiality statement and are transferred to duties that give them access to DHCS PHI, they must sign a confidentiality statement before access is granted. DHCS does not have a template confidentiality statement but can work with contractors to develop an acceptable statement if desired. While a confidentiality statement is not a specific federal requirement, DHCS is required under HIPAA to protect the confidentiality and integrity of its PHI and requiring employees to execute confidentiality statements is a reasonable measure to help achieve this goal.

Question 6: For Provision 3(C)(3)(b), new employees are often subjected to a background check conducted before being hired. Is the expectation to conduct an additional background check on new or existing employees? This would appear unreasonable in its request if additional background checks must be adhered to. This is not a state or federal requirement from a Security and Privacy perspective.

Answer: This Provision is not intended to impose the requirement to conduct a second background check in addition to one already required of new employees. It is intended to impose the requirement that a background check must be conducted for all employees who will have access to DHCS PHI. Although this is not a specific federal or state requirement, it is a reasonable security measure and one of DHCS' requirements under the contract.

Question 7: For Provision 3(C)(3)(c) some contracted entities currently utilize Pretty Good Protection (PGP) encryption software, PGP Corporation, which is on the State of California's Strategic Sourced Initiative Listing. However, in the future, if a software vendor utilized by a contracted entity does not appear on the CSSI listing, other reasonable options must be made available. Is DHCS the encryption software authority? What criteria are being utilized to determine approved software vendors? This should be technology neutral and scaleable to the size and scope of a particular organization. This is not a state or federal requirement.

Answer: DHCS approval is technology neutral; however, DHCS wishes to ensure that technical encryption solutions provide reasonable protection to its PHI data. The CSSI list has been provided as a convenience; it is not intended as an all-inclusive source of acceptable solutions. DHCS is unlikely to disapprove any solution that ensures encryption of all PHI data using industry standard encryption methods such as AES.

Question 8: Provision 3(C)(3)(d) contains language consistent with current industry security practices and federal requirements. However, how is "minimum necessary" being specifically defined? There is no state requirement.

Answer: Minimum necessary is defined consistently with its use in HIPAA as limiting the disclosure of PHI to the "minimum necessary to accomplish the intended purpose of the use, disclosure, or request." (45 CFR 164.502(b); see also 45 CFR 164.514(d).) It is a requirement of HIPAA that only the minimum necessary amount of PHI be disclosed.

Question 9: Provision 3(C)(3)(f) contains language consistent with industry current security practices and federal requirements. However, is this requirement referring to internal and external e-mails? The state requirement involved the Security Breach Notice regulation.

Answer: This requirement is specific to "external" in that it's applicable to any e-mail transported outside the internal, secure network.

Question 10: Provision 3(C)(3)(g) contains language consistent with industry best practices. This is an addressable federal standard and therefore the organization may:

- 1) Implement the specification if reasonable and appropriate
- 2) If implementing the specification is not reasonable and appropriate---document the rationale supporting the decision and implement an equivalent measure that is reasonable and appropriate and that would accomplish the same purpose, or
- 3) Not implement the addressable implementation specification or an equivalent alternative measure, if the standard could still be met and implementing the specification or an alternative would not reasonable and appropriate. This is not a state requirement.

Answer: The DHCS position is that there is no acceptable alternative to this requirement.

Question 11: Provision 3(C)(3)(h) contains language consistent with industry best practices. However, there are many Security patches given (e.g., Microsoft patches), and not all are applicable. What is the performance DHCS wants the plans to achieve? This is not a state or federal requirement.

Answer: DHCS recognizes that not all security patches may be applicable in a given situation. DHCS expects that the Contractor would assess which security patches are critical and applicable, and ensure they are applied within a reasonable timeframe. A recommended maximum timeframe for critical patches is two weeks.

Question 12: Provision 3(C)(3)(i) Password Management is an addressable specification in the Security standard. It calls for a covered entity to implement procedures for creating, changing, and safeguarding passwords. There is no need for the boilerplate contract to specify how to create passwords and even when to change passwords.

Answer: DHCS has an obligation to ensure reasonable security controls are in place to protect its PHI, which includes any passwords which could grant access to this PHI if compromised. While DHCS believes 60 days is a reasonable password change interval, DHCS' ISO will allow 90 days interval exceptions without prior approval.

September 29, 2009

Question 13: Provision 3(C)(3)(j) contains language that is inconsistent. On one hand, "all data must be wiped from systems when the data is no longer necessary;" however, within the same requirement, it states, "all DHCS data must be returned to DHCS when the data is no longer necessary." Which is it? There is no state or federal requirement.

Answer: The language to return data was removed from this document, so the requirement stands as is and all data must be wiped. It should be noted that paper containing DHCS PHI data must be shredded.

Question 14: Concerning Provision 3(C)(3)(j), the choice of how to comply with HIPAA specification on the destruction of PHI should be left to Plans. DHCS' choice of Department of Defense standards seem arbitrary and could result in costly implementation procedures. Just referring to Department of Defense standards is also not specific enough to enable Plans to easily locate the standards.

Answer: DHCS has an obligation to ensure its data is securely wiped. The DoD standard is widely accepted for this purpose, and is not an arbitrary selection. The particular standard referred to is DoD 5220.22-M and is supported by a wide variety of products. Other solutions should be submitted to the DHCS for review, and will be approved if DHCS finds no significant risks in the solution.

Question 15: Provision 3(C)(3)(k) is also prescription of solution. Plans should be allowed the choice.

Answer: DHCS has an obligation to ensure its PHI is protected if made available on the Internet through a remote access solution. DHCS is not requiring particular products, but is indicating that the method must be approved by DHCS ISO. The reference to CSSI is an aid intended to help in finding such solutions. DHCS ISO considers any solution using SSL or IPsec as meeting this requirement. Other solutions should be submitted to the DHCS for review, and will be approved if DHCS finds no significant risks in the solution.

Question 16: Provision 3(C)(4)(a) is a DHCS requirement. Are Plans in breach of contract if they use a 20 or 25 minute timeout setting? The CMS implementation specification is for a covered entity to have electronic procedures that terminate an electronic session after a predetermined time of inactivity. Why did DHCS choose 20 minutes?

Answer: Unattended, unlocked screens with DHCS PHI are a significant risk to DHCS' data. 10 to 20 minutes is the common range for screen saver timeouts, and DHCS requires the high end of this range. DHCS has not seen evidence of a 20 minute timeout being a significant inconvenience to end users. If this 20 minute timeout range provides a hardship to an organization, DHCS ISO will consider requests for up to 30 minutes, provided the organization can show strong physical security surrounding any workstations accessing DHCS PHI.

Question 17: Provision 3(C)(4)(b) is an addressable federal standard. This is not a state requirement. Additionally, would the warning banners need to be displayed on every page at the beginning of a user's system?

Answer: A warning banner must appear at least once prior to granting access to DHCS PHI. How this is implemented is up to the Contractor (e.g. during network logon or within an application).

Question 18: Provision 3(C)(4)(e) contains language that is consistent with industry best practices. This is an addressable federal standard. This requirement should be technology neutral due to the potential high cost involved. This is not a state requirement.

Answer: DHCS will not dictate a particular technology but requires Contractor ensure that the solution provides reasonable protection for DHCS PHI and leverages current best practices. Solutions using 128bit SSL, FTPS, or SFTP are acceptable.

Question 19: Provision 3(C)(4)(f) contains language that is consistent with industry best practices. This is an addressable federal standard. There are covered entities that may not have the technical expertise needed for a host-based intrusion detection and prevention system. This may also be cost-prohibitive. This is not a state requirement.

Answer: DHCS clarifies that "and" was intended rather than "or", e.g. intrusion detection is required only if a system which stores DHCS PHI is accessible via the Internet. Additionally, it should be noted that an appropriately configured network intrusion detection system would be considered equivalent to host based intrusion detection.

Question 20: Provision 3(C)(5)(b) indicates that "logs must be maintained for six years after the occurrence."

Answer: HIPAA requires a covered entity to implement policies and procedures to comply with the HIPAA privacy and security rules, and the covered entity must maintain these policies and procedures, in written or electronic form, until six years after the later of the date of their creation or last effective date. See 45 CFR 165.530(i) and (j). The requirement that log reviews be conducted is a procedure that helps ensure unauthorized access will be prevented or, if it does occur, will be detected in a timely manner. Keeping a record of the log reviews for six years documents that these reviews have been done.

Question 21: As for Provision 3(C)(7)(d), currently contracted entities utilize off-site storage of data and a signed business associate agreement governs the handling of PHI information with the off-site storage vendor. Would this suffice?

Answer: If the business associate agreement with the off-site storage vendor subjects the vendor to all the restrictions and conditions that apply to the Contractor, as required by

September 29, 2009

paragraph D on page 6 of the contract, the business associate agreement would be sufficient.

Question 22: For Provision 3(C)(7)(d), why is DHCS approval required to store information offsite? What are the criteria DHCS will use to approve or disapprove request?

Answer: The storage of information offsite increases the risk of unauthorized disclosures or loss of information. DHCS is requiring approval only when such removal is not under routine business purposes, which should have already been disclosed under section 2(C) "Prohibition of External Disclosures of Lists of Beneficiaries". DHCS approval criteria may include, but is not limited to, factors such as compliance with 3(D) "Contractor's Agents", general security of DHCS data, and compliance with any applicable regulations.

Question 23: Regarding Provision 3(C)(7)(f), most contracted entities could adhere to this practice but would need to ensure through a policy and procedure which states that large volume mailings of DHCS PHI shall be sent by secure, bonded courier with signature required on receipt and that disks and other transportable media sent through the mail must be encrypted. Would that suffice? This is not a state or federal requirement.

Answer: Pursuant to paragraph D on page 6, the Contractor must ensure that any agents, including subcontractors, agree to the same restrictions and conditions that apply to the Contractor. This is best accomplished by including the restrictions and conditions in the contract or agreement between the Contractor and agent or subcontractor. The Contractor must ensure that large volume mailings of DHCS PHI are sent by secure, bonded courier with signature required on receipt, and that disks and other transportable media sent through the mail or that otherwise leave the Contractor's site are encrypted. If adoption of a policy and procedure by the Contractor, agent or subcontractor is needed to achieve these measures, those steps should be taken.

Question 24: Provision 3(H)(1)(a) and (b) needs clarity. Is this PHI at the Contractor level only or does this include all subcontractors and agents? The current practice from the DHCS Privacy Officer and DHCS has been "within a 15 day" period of time. Is there a distinction between electronic, paper, oral and other media for adherence to this provision? Is it all the same for all forms of PHI; if not, what applies to what PHI medium?

Answer: DHCS must be notified when a breach is discovered at any level, including the Contractor, agent or subcontractor, and of any medium, including electronic, paper or oral. Notification must be immediate if the PHI was, or is reasonably believed to have been, acquired by an unauthorized person. In all other instances, including suspected security incidents, notification must be within 24 hours. The notification requirements are the same for all media, electronic, paper and oral.

Question 25: For Provision 3(H), what are the criteria for specifying 24 hour notification by e-mail or fax? Plans can be required to notify DHCS immediately upon discovery of breach

or suspected breach by telephone and within 10 days submit a written report that will address the elements stated in Provision 3(H)(2). The Cal Office of HIPAA Implementation (CalOHI) requires State agencies to immediately report a breach and then allows 10 days for State agencies to make a written report. The applicable CalOHI policy instructs any State department that is a covered entity or a business associate of a covered entity department to complete and submit a "HIPAA Supplemental Security Incident Report" form to CalOHI within 10 business days of becoming aware of an incident involving the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system containing electronic protected health information.

Answer: Plans are required to immediately notify DHCS when there is a breach in the security of PHI that is kept in computerized form if the PHI was, or is reasonably believed to have been, acquired by an unauthorized person. The criteria specifying 24 hour notification by e-mail or fax applies to suspected security incidents, intrusions or unauthorized use of disclosure of PHI in violation of the contract, or potential loss of confidential data affecting the Contract. The requirement of immediate notification with computerized PHI is reasonable and is consistent with other state law requirements because a breach of computerized PHI that is, or is reasonably believed to have been, acquired by an unauthorized person represents an immediate risk of identity theft or improper use of the disclosed information. Requiring a fax or e-mail in addition to a telephone call ensures that the report is received and documented. A security incident, such as a failure to properly encrypt e-mail transmissions or to lock up confidential information puts PHI at risk, but the risk is not as immediate as that created when computerized information is acquired by an unauthorized person. Permitting notification of security incidents by e-mail or fax within 24 hours is reasonable because of the lesser risk created by this type of incident.

Requiring an immediate investigation and a report within 72 hours of the discovery addressing the elements stated in Provision 3(H)(2) enables DHCS and the entity reporting the breach to determine how serious the breach is and to start taking action to mitigate possible harm as soon as possible. DHCS recognizes that 72 hours may not be sufficient time to verify all the facts of an incident. However, DHCS believes that it is important to get information on the elements listed in Provision 3(H)(2) as soon as possible so that immediate action can be taken to protect the beneficiaries whose information has been improperly disclosed. A full investigative report is not required until 10 working days after discovery of the incident, which gives the entity two weeks to conduct an investigation. DHCS feels that these timeframes are reasonable and will help ensure that breaches are reported and mitigated in a timely, responsible manner.

Question 26: As for Provision 4(B), Contracted Entities' General Counsels and their respective Legal Departments may have final commentary on the adherence of litigation and administrative proceedings.

September 29, 2009

Answer: DHCS understands that, in the event of litigation or administrative proceedings, the assistance and cooperation to be provided by the Contractors, agents and subcontractors may include the assistance of the General Counsels and Legal Departments of the contractors, agents or subcontractors.

CONTRACT SECTIONS ALREADY REMOVED

The following sections have already been removed from Exhibit G based upon DHCS' agreement to do so following and pursuant to feedback received from health plans.

- Provision 3(C)(4)(a) – System Architecture
- Provision 3(C)(4)(f) – Input Controls

FUTURE UPDATES

Additionally, DHCS agrees to the following changes, which will be updated in future amendments:

- Provision 1(B) will be changed to read: "DHCS desires to protect the privacy and provide for the security of PHI disclosed, created, received, maintained or transmitted on behalf of DHCS pursuant to this Contract."
- Provision 2(B)(2) will be changed to read: "Data aggregation means the combining of PHI created or received by the Contractor on behalf of DHCS with PHI received by the Contractor in its capacity as the Contractor of another covered entity, to permit data analyses that relate to the health care operations of the Medi-Cal program."
- Provision 2(B)(2) which includes the definition of aggregation can be modified by using the following language: "received by the Contractor in its capacity as the Contractor of another covered entity from another covered entity."
- Provision 3(C)(4)(f) will replace or with and: "All systems that are accessible via the Internet and store DHCS PHI..."

If you have any questions or require additional information, please contact your Contract Manager.

Sincerely,



Tanya Homman, Acting Chief
Medi-Cal Managed Care Division