DEPARTMENT OF
BUDGET & MANAGEMENT

MARTIN O'MALLEY
Governor

ANTHONY BROWN
Lieutenant Governor

T. ELOISE FOSTER
Secretary

DAVID C. ROMANS
Deputy Secretary

Q & A #5
to
REQUEST FOR PROPOSALS (RFP)
DPSCS INMATE MEDICAL HEALTH CARE AND UTILIZATION SERVICES
SOLICITATION NUMBER DPSCS Q0012013
MARCH 7, 2012

Ladies and Gentlemen:

The following questions, for the above referenced RFP, were received by e-mail and are being answered and posted for all Offerors. The numerical sequencing begins with question #319; questions #1 through #4 were answered in Q&A #1, issued on July 21, 2011, questions #5 through #276 were answered in Q&A #2, issued on November 4, 2011, questions #277 through #318 were answered in Q&A #3, issued on November 12, 2011 and questions #319 through #329 were answered in Q&A #4, issued on November 15, 2011:

330. Question**:** *Amendment Pg. 4, Section 3.73.2.1*: Does the annual audit apply to the current NextGen system? If so, how will the Contractor's third party audit firm complete the audit since the NextGen application sits within the State's Data Center? Will appropriate access be granted to the third party auditor?

Answer: No, the requirements of § 3.73.2.1 do not apply to the NextGen System itself as long as the NextGen System is hosted and controlled by DPSCS. However, as per the answer to question #3, below, the Contractor may still have to include in a SOC 2 audit how it will maintain the security of information accessed via the NextGen System, even if the NextGen System is hosted by DPSCS.

331. Question**:** *Amendment Pg. 4, Section 3.73.2.1*: If the DPSCS decides to move forward with the optional EHR, will the Contractor have to provide SOC 2 Reports for the NextGen MD supported system and the potentially hosted optional EHR as transition occurs?

Answer: As per the answers to questions #1 & 3, the Contractor may have to provide SOC 2 reports concerning any personally identifiable information contained in any database that it either hosts, or to which it has access, directly

or via an entity operating on its behalf. The scope and complexity of its SOC 2 report will be greater for databases hosted by the Contractor or an entity operating on its behalf than if there is only access to data in a system hosted by the State.

332. Question**:** *Amendment Pg. 4, Section 3.73.2.1:* Does the SOC 2 audit only apply to Medical Records Systems?

Answer: The answer to this question depends upon what "medical records systems" are considered to be. While the SOC 2 audit does apply to medical records of Inmates, it also applies to any personally identifiable information of individual Inmates or relatives, friends or others associated with Inmates. For instance, non-medical information such as Inmates' Social Security numbers, date of birth, last known address, financial circumstances, such as eligibility for medical assistance or coverage by private medical insurance, names, addresses, phone numbers, etc. of relatives, friends or contacts that might be contained in discharge planning records or in searches for third party responsibility for medical expenses should all be covered under a SOC 2 audit. If any personally identifiable information that in any way pertains to an Inmate or anyone associated with an Inmate that is maintained or accessible by the Contractor under this Contract is considered to be within the Contractor's medical records systems, the answer to this question would be yes. If such information is considered to be beyond the scope of the Contractor's medical records systems, the answer would be no.

The bottom line is that a SOC 2 audit may have to cover any personally identifiable information of Inmates or individuals associated with Inmates that the Contractor either maintains in any database hosted by itself or any non-State entity, or to which the Contractor or any non-State entity operating on behalf of the Contractor has access, even if the information is maintained in a State controlled database.

However, it is important to remember that there are a number of databases that the Contractor is required to maintain under the Contract. Regardless whether the primary repositories of personally identifiable information are DPSCS hosted databases such as NextGen or OCMS, the Contractor may still have to include standalone Contractor hosted databases in its SOC 2 audit report.

Examples of such required Contractor maintained databases are:

The sick call slips and referral log required by § 3.28.5 if such information can not be maintained in the EHR.
The log required by § 3.29.1.1e.
The chronic care clinic attendance database required by § 3.30.1.2.

Further, in providing various reports required under the Contract the Contractor must compile at least some personally identifiable information, presumably in a temporary or permanent file it maintains, such as the monthly:

PPD positives report required by § 3.26.2.1.4
StateStat report as per Attachment Q
TB/HIV/STD report required by § 3.26.2.3.4
Periodic Physical Examination report required by § 3.27.2.

Finally, the electronic transmission of digital radiology and the use of telemedicine are additional situations when the Contractor will have individually identifiable Inmate medical information under its control, hence additional circumstances that may have to be covered by the SOC 2 audit report.

333. Question**:** *Amendment Pg. 5, Section 3.73.2.1.1:* Please define in more detail what is expected in the SOC 2 Audit Plan due within 40 days.

Answer: Based upon the answer to the above question, the Contractor in its SOC 2 plan must detail how it will maintain the confidentiality of such information. It addition, as per requirements of § 3.73.2.2, the Plan should identify how the Contractor will notify DPSCS and affected individuals in the case of a security breach and steps it will take to minimize the effect of any such breach and prevent recurrence, and its proposed disaster recovery system.

However, in many, if not most circumstances the information that would be covered by a SOC 2 audit is information covered by HIPPA. Hence, the Contractor may have few or no new requirements pertaining to a SOC 2 audit than it is already required to do under HIPPA provisions. Moreover, as per § 3.73.2.1 the Contractor's current security audit procedures may be sufficient so that a SOC 2 audit is not required. Accordingly, the SOC 2 audit plan may simply be a description of the security auditing the Contractor is currently performing, and pledges to continue to perform.

334. Question**:** *Amendment Pg. 5, Section 3.73.2.1.3:* To clarify: is the first SOC 2 Report, assuming the start date of July 1, 2012, due within 30 days of June 30, 2013?

Answer: Yes.

Should you require clarification of the information provided, please contact me at (410) 260-7374 as soon as possible.

Date Issued: **March 7, 2012**

By: Andrea R. Lockett
<signed>
Procurement Officer