Cloud Computing Toolkit

Use Case: Use of Cloud for Healthcare Organization's Remote Backup of Confidential Information

By Adam H. Greene, JD, MPH and Lee Kim, JD, FHIMSS

Many healthcare organizations are outsourcing to the cloud. As with all IT solutions, one size does not fit all. This use case may be used as a guide to determine if remote backup of confidential information to the cloud is appropriate for your organization. The confidential information may include electronic protected health information ("ePHI") or other sensitive and/or proprietary information.

1. Identify all ePHI and other confidential information that needs to be backed up.[1,2] Your healthcare organization needs to create an inventory of all ePHI and other confidential information that needs to be backed up. The ePHI may be stored in files, databases, or applications, including cloud based applications. With respect to a cloud based application, the vendor may already have the capability to back up the information to the cloud. However, the organization should still consider how it will respond if the data is unavailable from the vendor for some reason, such as a contractual dispute. Note: While this use case focuses on ePHI and other confidential information, the backup of this data should be part of a more general business continuity plan, which ideally includes classification of all data and back up of all critical data.

2. Identify whether your organization has the infrastructure to support a cloud-based solution for the backup of some or all confidential data. Consider factors such as your network bandwidth, uptime, connectivity, and redundancy in the event of a natural disaster or other incident. Be sure to review your healthcare organization's general business continuity plan.

3. Consider the general benefits and drawbacks of cloud-based versus local backup. This step can be completed in conjunction with the next step (i.e., selection of cloud provider and related due diligence), as the advantages and disadvantages may differ significantly among cloud providers.

    - Consider what type of cloud-based backup would be feasible (e.g., SaaS, IaaS, or PaaS). For example, a Software-as-a-Service (SaaS) cloud provider may offer backup of the application data. This may be the simplest option, but likely provides the least amount of control and customization. More sophisticated healthcare organizations may consider using a Platform-as-

[1] See NIST SP 800-34 Rev. 1 for more information on contingency planning.
[2] The organization may identify some ePHI that is reasonable to not backup (e.g., because it is not critical to ongoing patient care or business functions), in which case the organization may document the basis for why such ePHI is not backed up.

a-Service (PaaS) or Infrastructure-as-a-Service (IaaS) cloud provider to create a more customized backup solution.

- Consider whether the healthcare organization will use a public cloud, a private cloud, or a hybrid cloud solution. In the event of a private cloud solution, will the healthcare organization host the cloud itself or rely on a third party?[3]

- Consider the costs involved with the cloud-based vs. local backup. What are the costs, including staff time, to locally back up data, transfer the media to a secure location, and restore the data in the event of a disaster? In comparison, what are the costs to have data backed up to a cloud provider, maintained with that cloud provider, and restored from that cloud provider?

- Consider the impacts on information security for cloud-based vs. local backup. Will the cloud provider offer greater administrative, physical, and technical safeguards than what is available through local backup? Will each option include encrypting the data in transit and at rest, and maintaining appropriate controls with respect to the encryption keys? Which option provides greater information security expertise to maintain the security of the data? These considerations may differ significantly based on the type of cloud model that would be deployed (e.g., public vs. private).

- Consider the time to restore data in the case of a natural disaster or other incident for cloud-based vs. local backup. As part of contingency planning, your organization may conduct a business impact assessment by considering factors such as, but not limited to, maximum tolerable downtime ("MTD"), recovery time objective ("RTO"), and recovery point objective ("RPO") to help determine which option would be best for your healthcare organization.[4]

- Consider the impact of the geographic location of cloud-based vs. local backup. If backups are performed locally, how far away from the healthcare organization are they maintained? Or, if your healthcare organization is a larger organization, are facilities sufficiently dispersed that you can maintain a backup for each facility at another facility's location with limited risk that the same incident will impact multiple locations? Will a cloud-based solution offer reduced risk by maintaining the backup data substantially further away from the primary site?

- Consider whether there are greater or lesser privacy and information security concerns with using a cloud-based solution compared to a local backup solution. If a third party cloud provider is used, will the data be encrypted in a manner that the information is not accessible to the cloud provider? Or will the use of the cloud provider increase the number of persons who have access to the data? Will the use of a cloud provider introduce the risk that law enforcement or another third party could view your data without your knowledge? Or will the use of a cloud provider improve privacy and information security and significantly reducing the

[3] See HIMSS Cloud Computing Definition & Background paper for more information about different types of solutions.
[4] See NIST SP 800-34 Rev. 1 for more information on these recovery measures.

risk of a breach of confidentiality? In an electronic environment, one needs to keep information secure in order to keep it private.[5]

- Consider costs associated with using a third party provider or entity for cloud-based backups or local backups. What are the additional costs in the event that the relation with the third party is terminated (e.g., time and costs to ensure the return or destruction of the information from the first vendor and implement a new solution with a new vendor)?

4. If you have determined that cloud-based backup is the best solution for your organization, identify suitable cloud provider(s) (if a third party cloud provider will be used) and conduct appropriate business and technical due diligence.

- What assurances do you have that the cloud provider has sufficient information security in place? Is the cloud provider's information security independently assessed by a third party on a periodic basis? Can the cloud provider provide documentation or a summary of such assessment(s)? Alternatively or in addition to such an assessment, has the cloud provider provided information about their security practices such as by answering a security questionnaire? [6] Will information security be guaranteed through the master services agreement, service level agreement (SLA), or other means? How are they responding to the continually increasing threat environment (e.g., a proactive penetration testing program)?

- Which cloud provider offers the best combination of cost, reliability, information security, and customer and technical support for your healthcare organization?[7]

- What is the reputation and track record of the cloud provider? Has the cloud provider been around for five years or more? Consider resources that assess the organization's financial viability (e.g. financial rating, customer references, etc.). Know who the true owner is of the cloud provider—is it a standalone company or owned by another entity?

- Will the cloud provider subcontract the hosting of the data (e.g., to an IaaS provider) or maintain the data at a third party's data center? If so, what is the reputation and track record of the subcontractor? Know the true owner of the data center-- is it a standalone company or owned by another entity? Also know where the data center is located geographically.

- Which service levels are guaranteed or otherwise promised (i.e., in a service level agreement) by the cloud provider? What are the remedies (e.g. credits, penalties, or otherwise) if the cloud provider fails to meet the promised service levels? Can the contract be terminated if service levels repeatedly are not met?

- If the agreement is terminated, how will the information be returned or destroyed? If returned, what will be the format? Are there charges for return of data to your healthcare organization or migration

[5] See HIMSS Cloud Computing Privacy and Security 101 paper for additional discussion of potential privacy and security advantages and disadvantages of using cloud-based services.
[6] See HIMSS Questions to Ask Potential Cloud Providers and Health Care Cloud Coalition's Draft Cloud Security Assessment for sample information security due diligence questions and topics.
[7] See Hidden Pitfalls with Cloud, Mobile Technology and Mobile Data, HIMSS14 (Feb. 24, 2014) for additional tips on conducting cloud due diligence.

to another cloud provider which your healthcare organization has chosen? If the data is destroyed, how will the information be destroyed and what documentation of destruction, if any, will be provided? Is the cloud provider willing to provide a certificate of destruction of the data? If neither return nor destruction of the data is possible, how does the cloud provider intend to continue to keep the data secure?

5. Enter into a HIPAA business associate agreement with the cloud provider if it will be creating, receiving, transmitting, or maintaining ePHI.[8] If the cloud provider would be a "qualified service organization" under the Confidentiality of Alcohol and Drug Abuse Patient Records at 42 C.F.R. Part 2 (applicable to federally-assisted alcohol and drug abuse treatment programs), then ensure that the agreements (e.g., the primary agreement, the business associate agreement, or the service level agreement) include the terms required by this rule too. Also, the agreements should be consistent with any other applicable laws, such as, but not limited to, state confidentiality and breach notification laws.

6. Implement cloud-based backup. Create/revise data backup and disaster recovery plans (required by 45 C.F.R. § 164.308(a)(7)(ii)(A) and (B) of HIPAA) tailored to the use of a cloud-based backup. Ensure that staff is available, including essential and contingency staff who are knowledgeable about how to perform disaster recovery after a natural or manmade disaster (which may include a cyber-attack). As noted above, the backup and restoration of ePHI and any other confidential information should be part of larger contingency planning, and your organization should ensure that all backup and restoration processes meet the organization's business and technical objectives.[9]

7. Conduct periodic disaster recovery testing and verification Revise data backup and disaster recovery plans as needed as a result of testing and verifying these plans. In addition, periodically test and verify data backup and recovery to ensure backups are complete, available, have integrity, and that essential and contingency staff continues to know how to restore data after an incident makes primary data unavailable. Consider testing a simulated failure of the cloud-based backup solution to make sure that your organization's contingency plan addresses such a risk.[10]

[8] See HIMSS Navigating HIPAA While Moving to the Cloud paper for more information.
[9] See NIST SP 800-34 Rev. 1 for more information on contingency planning.
[10] See 45 C.F.R. § 164.308(a)(7)(ii)(C).