HIPAA on Amazon Web Services

Thank you for joining AWS' HIPAA Business Associate program. We're happy to have established a Business Associate Agreement (BAA) with The Regents of the University of California on behalf of the University of California Office of the President and want to provide you with a reference guide to help you get started.

Review the BAA configuration requirements with your team

Prior to doing any HIPAA-related work in your AWS account, read your BAA agreement and enterprise agreement and make sure your team understands and can address the following key points. If you are unsure of what an AWS term means or would like guidance, please reach out to your account manager and solutions architect.

- ✓ Review your local organizational policies regarding security and auditing requirements to comply with HIPAA regulations and BAA requirements.
- ✓ Become familiar with the HIPAA eligible services provided by AWS.
- ✓ Review and understand the AWS Shared security model.
- ✓ Review BAA section 4.3 regarding your data processing, storage and transmission requirements on dedicated instances and encryption of PHI.
- ✓ Ensure you have all necessary consents for PHI you may place on AWS.

Identify your AWS HIPAA Accounts

Each AWS account you wish to have covered under the BAA must be registered with AWS. Review the accounts that have or will likely have PHI resource needs. This is also a good time to review how this process will flow in the future as new accounts are requested to be added.

- ✓ Identify all of your accounts intended to be covered under the BAA.
- ✓ Ensure that account contact information is accurate
- ✓ Consider entering an alternate security point of contact

Register your HIPAA accounts

All AWS accounts that will contain PHI must be registered with AWS in order to be covered under the BAA. This is a critical responsibility as noted in the BAA in section 4.1. Please send a request to your AWS Account Manager (see contact info on next page) with the following information:

- ✓ AWS account ID and whether the ID is an addition or removal from the BAA.
- ✓ The name of the UC campus with which the account ID is primarily associated.
- ✓ Once AWS has replied back that the request has been fulfilled, retain this email as confirmation of your request being completed.

Architect and develop your HIPAA solution in AWS

Review relevant developer and technical safeguard materials for implementing your HIPAA solution.

- ✓ Review the NIST 800-66 resource guide.
- ✓ Review AWS HIPAA whitepaper as well as any relevant AWS product documentation.
- ✓ Consider leveraging AWS solutions architects for review of your design and implementation. You may contact your AWS account manager to access AWS solution architects, free-of-charge.

Deploy and operate your HIPAA solution in AWS

You should now be able to start deploying your HIPAA workload on AWS. Please keep in mind that HIPAA regulations may change and that AWS may update our HIPAA program from time to time so it's important to keep up to date on the latest requirements that may impact your HIPAA solution.

Contacts:

- UCOP Cloud services guidance
- AWS Account Reps
  - Matt Jamieson: mattjam@amazon.com, 650-248-1793
    - UC Agriculture and Natural Resources
    - UC Berkeley
    - UC Davis
    - UC Merced
    - UC Office of the President
    - UC Santa Cruz
      UC San Francisco
  - Heather Matson: hmatson@amazon.com, 858-776-6913
    - UC Irvine
    - UC Los Angeles
    - UC Riverside
    - UC Santa Barbara
    - UC San Diego

Resources:

- AWS HIPAA Compliance
- AWS HIPAA HITECH Compliance Whitepaper (pdf)