AWS Encryption:

Most of the information I found was straight from the AWS Relational Database System guide. If you scroll down a bit in this link, you'll find the "Overview of encrypting Amazon RDS resources", which details how AWS encrypts data and options with their KMS (key management service).

Customer keys and AWS keys

The KMS keys that you create are customer managed keys. AWS services that use KMS keys to encrypt your service resources often create keys for you. KMS keys that AWS services create in your AWS account are AWS managed keys. KMS keys that AWS services create in a service account are AWS owned keys.

Type of KMS key	Can view KMS key metadata	Can manage KMS key	Used only for my AWS account	Automatic rotation	Pricing
Customer managed key	Yes	Yes	Yes	Optional. Every year (approximately 365 days)	Monthly fee (pro-rated hourly) Per-use fee
AWS managed key	Yes	No	Yes	Required. Every year (approximately 365 days)	No monthly fee Per-use fee (some AWS services pay this fee for you)
AWS owned key	No	No	No	Varies	No fees

AWS services that integrate with AWS KMS differ in their support for KMS keys. Some AWS services encrypt your data by default with an AWS owned key or an AWS managed key. Some AWS services support customer managed keys. Other AWS services support all types of KMS keys to allow you the ease of an AWS owned key, the visibility of an AWS managed key, or the control of a customer managed key. For detailed information about the encryption options that an AWS service offers, see the *Encryption at Rest* topic in the user guide or the developer guide for the service.

There is also a simple section (Encrypting a DB instance) that **guides the user in encrypting a new DB instance. Basically, when you create a new DB instance, you can choose the "Enable encryption" option in the Amazon RDS console**. If we use the create-db-instance AWS CLI command to create an encrypted DB instance, we can set the --storage-encrypted parameter. If we use the CreateDBInstance API operation, we can set the StorageEncrypted parameter to true. There is also an extensive guide that details AWS's RDS capabilities, one of which relating to encryption.

Encryption	**Enable Encryption** to enable encryption at rest for this DB instance.
	For more information, see Encrypting Amazon RDS resources.
		CLI option:
		`--storage-encrypted`
		`--no-storage-encrypted`
		RDS API parameter:
		`StorageEncrypted`

Finally, there are some details about some limitations with encryption in Amazon's RDS DB encryption. Note: a database snapshot is a read-only, static view of an SQL Server database.

- You can only encrypt an Amazon RDS DB instance when you create it, not after the DB instance is created.

- However, because you can encrypt a copy of an unencrypted snapshot, you can effectively add encryption to an unencrypted DB instance. That is, you can create a snapshot of your DB instance, and then create an encrypted copy of that snapshot. You can then restore a DB instance from the encrypted snapshot, and thus you have an encrypted copy of your original DB instance. For more information, see Copying a DB snapshot.

- You can't turn off encryption on an encrypted DB instance.

- You can't create an encrypted snapshot of an unencrypted DB instance.

- A snapshot of an encrypted DB instance must be encrypted using the same KMS key as the DB instance.

- You can't have an encrypted read replica of an unencrypted DB instance or an unencrypted read replica of an encrypted DB instance.

- Encrypted read replicas must be encrypted with the same KMS key as the source DB instance when both are in the same AWS Region.

- You can't restore an unencrypted backup or snapshot to an encrypted DB instance.

- To copy an encrypted snapshot from one AWS Region to another, you must specify the KMS key in the destination AWS Region. This is because KMS keys are specific to the AWS Region that they are created in.

- The source snapshot remains encrypted throughout the copy process. Amazon RDS uses envelope encryption to protect data during the copy process. For more information about envelope encryption, see Envelope encryption in the AWS Key Management Service Developer Guide.

- You can't unencrypt an encrypted DB instance. However, you can export data from an encrypted DB instance and import the data into an unencrypted DB instance.