Data from third-party apps that use iCloud

iCloud Backup is also enabled to help ensure you have a current backup of the data on your device in case you need to replace or restore it.

Your Apple ID includes the information you use to sign in, as well as all the contact, payment, and security details, such as trusted phone numbers or security questions, that you use across Apple services.

Certain data, including your contacts, calendars, photos, documents, health, activity, and other app data, will be sent to Apple to store and back up on your behalf.

Your Apple ID account information will be used with each service, and certain data from your device, including your selected profile photo, your contacts, calendars, photos, documents, health, activity, Safari tabs, and other app data, will be sent to Apple to store and back up on your behalf.

When processing data stored in a third-party data center, encryption keys are accessed only by Apple software running on secure servers, and only while conducting the necessary processing.

For more information on iCloud Data Security, visit support.apple.com/kb/HT202303.

Both Apple and third-party data centers may be used to store and process your data.

This means that, by design, only you can access this information, and only on devices where you’re signed in to iCloud.

In addition, your device will be associated with your Apple ID to provide you with better service and support.

When you use Find My, your device’s location, as well as information about your device and your account will be sent to and retained by Apple so we can provide you with the service.

iCloud Keychain uses end-to-end encryption and is designed so that only you can access this information and only on devices where you’re signed in to iCloud.

Apple retains your device’s name, serial number, and other hardware identifiers to provide you with better service and support, including as a convenience to display the warranty status of your device and to check your eligibility for service offers when you activate a device.

For certain information, Apple uses end-to-end encryption.

Otherwise, the backup data will be retained for up to 180 days.

It can also store the account information you use for Mail, Contacts, Calendar, Messages, Facebook, Twitter, LinkedIn, and other internet accounts and automatically add this information to all of your devices.

iCloud Backup

When you use iCloud Backup, your backup may include photos, videos, messages (iMessage, SMS, and MMS), Health and other app data, location settings (such as location-based reminders that you have set up), Visual Voicemail, device settings, device characteristics, and other data from your iOS or iPadOS device depending on your Settings.

No one else, not even Apple, can access your iCloud keychain data.

You can adjust which iCloud features are enabled and what data is sent to iCloud from Settings on your device at any time.

iCloud Data Security

iCloud protects your information by encrypting it when it’s in transit, storing it in iCloud in an encrypted format, and using secure tokens for authentication.

Sharing Data with iCloud