Seed Phrase Planning for Incapacity and Recovery

November 13, 2026 · Document #427 · bip39-phrase.com

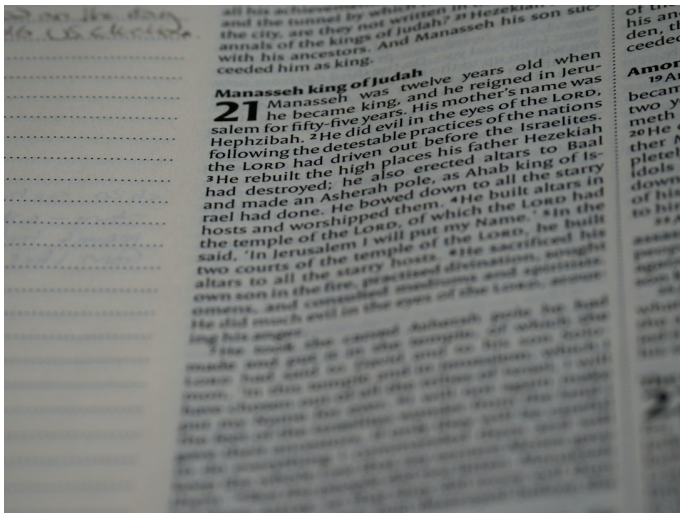


Photo by Brett Jordan on Unsplash

Plan wallet access for illness or incapacity with legal authority, separate care funds, shared signing and a recovery procedure.

Contents

Plan for care while you are alive	2
Match legal authority with technical access	2
Limit access through wallet design	3
Write and rehearse the procedure	3
FAQ	4
Sources	4
Example BIP39 word sequences	4
Reading a BIP39 phrase	5
See also	6

A seed phrase sealed with instructions to open it after your death cannot pay for care while you are alive. Dementia, a coma or an extended hospital stay calls for a plan that works when you cannot operate your wallet, preserves your ownership and allows you to resume control if you recover.

Plan for care while you are alive

An incapacity plan needs an activation process, money for ongoing expenses and a recovery procedure. A death plan concerns estate administration and distribution. In the United States, an agent's authority under a power of attorney ends at death; naming someone executor does not itself authorize them to manage your finances during your lifetime. ([files.consumerfinance.gov](https://files.consumerfinance.gov/f/documents/cfpb_msem_national_agents_guide.pdf))

Design for three situations: temporary inability to use devices, inability to communicate decisions, and progressive loss of decision-making capacity. Hospitalization alone should not automatically release every secret. Someone recovering from surgery may only need help paying bills; someone with dementia may need continuing financial management.

Write down which expenses should continue, who coordinates care and how much money should be available immediately. For example, choose a separate care reserve covering three months of expected costs, then specify how further funding should be requested. Treat that amount as a planning choice, not a universal recommendation.

Match legal authority with technical access

A **durable financial power of attorney** can authorize an agent to act and remain effective through incapacity. Durability concerns whether authority survives incapacity; it does not, by itself, determine when authority begins. Activation rules, permitted powers and execution requirements depend on local law. Arrange this while you have the required legal capacity. ([consumerfinance.gov](https://www.consumerfinance.gov/ask-cfpb/what-is-a-power-of-attorney-poa-en-1149/))

Ask a local estate-planning lawyer to address self-custodied assets explicitly: accessing devices and backups, signing transactions, selling assets for care, paying fees and keeping records. Specify whether gifts, loans, staking or other discretionary activity are prohibited. Name a successor agent and establish how incapacity and recovery will be documented.

A power of attorney supplies legal authority; it cannot reconstruct missing keys. Conversely, possessing signing material can enable transactions without establishing lawful authority. Bitcoin validates the applicable spending conditions, including required signatures; it does not assess a power-of-attorney document or medical evidence. Your access procedure must connect those separate systems. ([files.consumerfinance.gov](https://files.consumerfinance.gov/f/documents/cfpb_msem_national_agents_guide.pdf); [developer.bitcoin.org](https://developer.bitcoin.org/devguide/transactions.html))

Require records of each transaction's purpose, amount, fees and destination. The CFPB identifies acting in the owner's interests, managing carefully, separating property and maintaining records as core duties of an agent. ([files.consumerfinance.gov](https://files.consumerfinance.gov/f/documents/cfpb_msem_national_agents_guide.pdf))

Limit access through wallet design

A BIP39 mnemonic, together with a passphrase if one is used, derives a seed used to generate wallet keys. Giving someone those secrets for a conventional single-signature wallet provides broad signing capability across its derived accounts. A written spending limit does not change that cryptographic capability. ([github.com](https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki))

Consider these arrangements:

- Separate care wallet: Generate an independent seed and fund only the intended reserve. Give the agent access to that wallet. Another account under the main seed does not isolate funds from someone holding that seed. ([github.com](https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki))
- Bitcoin multisignature reserve: Use a tested `2-of-3` arrangement with one key held by you, one by your agent and one by an independent reviewer. The agent and reviewer can act while you are unavailable; neither can spend alone if each holds only their own key. Any two key holders can nevertheless authorize spending the entire balance. Basic multisignature enforces a signature threshold, not monthly allowances or approved expenses. ([github.com](https://github.com/bitcoin/bips/blob/master/bip-0383.mediawiki))
- Observation without signing: Share a public-only wallet export when the task is checking balances or preparing reports. Extended public keys can expose associated transaction activity, so treat them as sensitive financial information. They do not themselves supply spending keys. ([github.com](https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki))

BIP39 derives a seed from any passphrase without checking whether it is the intended one. Different passphrases generally produce different wallets, although text that becomes identical under BIP39’s Unicode normalization produces the same result. A passphrase adds no permission level, spending limit or expiration date. If its only correct copy exists in your memory, incapacity can defeat the recovery plan. ([github.com](https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki))

Write and rehearse the procedure

1. Prepare an inventory identifying networks, wallet software, devices and backup locations. Record derivation paths and, for multisignature, the public wallet descriptor and cosigner information needed for reconstruction. Keep private keys, seed phrases and passphrases separately. Public descriptors can also reveal sensitive financial information. ([github.com](https://github.com/bitcoin/bips/blob/master/bip-0380.mediawiki))
2. Document who verifies activation, who releases each item and who approves reserve replenishment. Include an alternative if a participant is unavailable.
3. Rehearse recovery with a separate, minimally funded wallet. Have the intended helpers complete the process without relying on your memory or improvisation.
4. Define recovery steps: reconcile spending, reassess authority and replace exposed signing material. Revoking legal permission does not erase copied keys; restoring exclusive control may require moving funds to a newly secured wallet. ([github.com](https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki))
5. Review the procedure after changes to health, relationships, wallets or backup locations.

FAQ

Can my agent recover funds using only the legal document?

The document cannot derive private keys. For self-custodied funds, the agent also needs an authorized, workable signing or recovery process. ([github.com](https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki))

Can I give someone only part of my seed phrase?

Missing words do not create a spending permission or a reliable access boundary; depending on how much is missing, someone may be able to reconstruct them. Prefer a separate funded wallet or a tested signature threshold for limited access. ([github.com](https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki))

What if I recover after access was activated?

Follow the documented return-of-control process, review transactions and replace any signing secrets whose continued possession by others is unacceptable. ([github.com](https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki))

Sources

- CFPB: Help for agents under a power of attorney (files.consumerfinance.gov)
- CFPB: What is a power of attorney (POA)? (www.consumerfinance.gov)
- Bitcoin Developer Guide: Transactions (developer.bitcoin.org)

> Continue reading on bip39-phrase.com: How to Store a Seed Phrase: Paper, Steel and Safe Locations
> More on this topic: Seed Phrases

Example BIP39 word sequences

Randomly generated sequences of words from the BIP39 English wordlist. None of them passes the BIP39 checksum, so no wallet will accept them: they show the format only. Never store funds with a phrase you found in a document.

Example 1

1	flee	2	cushion	3	company
4	milk	5	lab	6	release
7	office	8	raven	9	surprise
10	come	11	physical	12	prevent

Example 2

1	squeeze	2	brisk	3	small
4	ten	5	idle	6	people
7	syrup	8	discover	9	father
10	science	11	steak	12	flat

Example 3

1 rescue	2 indoor	3 window
4 destroy	5 sphere	6 dinner
7 sheriff	8 blur	9 security
10 remember	11 eager	12 street

Example 4

1 hole	2 bind	3 ceiling
4 size	5 car	6 dolphin
7 six	8 again	9 control
10 coyote	11 version	12 horse

Example 5

1 relax	2 night	3 base
4 economy	5 radar	6 play
7 tomato	8 scissors	9 buddy
10 child	11 carbon	12 click

Example 6

1 word	2 junior	3 napkin
4 milk	5 actress	6 onion
7 rare	8 reunion	9 law
10 two	11 rhythm	12 inspire

Example 7

1 ensure	2 genuine	3 error
4 broccoli	5 debate	6 mind
7 husband	8 hotel	9 wrap
10 flame	11 lift	12 like

Example 8

1 evil	2 gas	3 stereo
4 bronze	5 genuine	6 radar
7 faint	8 absent	9 enemy
10 flat	11 bachelor	12 try

Reading a BIP39 phrase

Every word stands for an 11-bit number: its position in the 2048-word list, counted from 0. Here is Example 1 decoded word by word. Each word links to its page on bip39-phrase.com, where the list is numbered from 1.

#	Word	Index (0-2047)	Word no.	11 bits
1	flee	710	711	01011000110
2	cushion	435	436	00110110011
3	company	372	373	00101110100
4	milk	1124	1125	10001100100
5	lab	992	993	01111100000
6	release	1449	1450	10110101001
7	office	1228	1229	10011001100
8	raven	1427	1428	10110010011
9	surprise	1747	1748	11011010011
10	come	368	369	00101110000
11	physical	1311	1312	10100011111
12	prevent	1362	1363	10101010010

The 12 words carry 132 bits: 128 bits of entropy followed by a 4-bit checksum. The checksum must equal the first 4 bits of the SHA-256 hash of the entropy.

`Entropy (hex): 58c6ccba4647c16a666593da65c28fd5`

This sequence ends in the checksum bits 0010, but SHA-256 of its entropy starts with 1010, so wallets reject it as an invalid phrase. That is the point of the checksum: about 15 of every 16 random or mistyped sequences fail it.

See also

- BIP-39 Seed Phrases: The Most Dangerous Backup You'll Ever Own · June 18, 2025
- Letter of Instruction for BIP39 Seed Phrases · June 14, 2026
- Picking a Seed Phrase Executor: Trust Before Skill · October 27, 2026
- Twelve Words to Rule Your World: The Seed Phrase as Digital Sovereignty · June 17, 2025

Educational document. The example sequences are random and fail the BIP39 checksum: they are not wallets and must never hold funds. Security notes: bip39-phrase.com/security/