# Secure Digital Planning for Life Events

Life changes in both noticeable and subtle ways, such as shared responsibilities, adjusted habits, or routines that no longer function as they once did. These shifts affect how things are managed, and different people may step into roles you previously handled on your own, whether a family member, a close friend, or a professional advisor.

Preparing for these moments isn't about anticipating the worst; it's about being kind to ourselves and others. Life can bring many challenges—a hectic schedule, a medical appointment, travel, recovery, or times when we can't be there to walk others through the details. By ensuring that everyone has the information they need, we empower them to step in with confidence and respect during those times. It's genuinely about supporting one another in the journey ahead.

Since so much of daily life now happens digitally, it's natural for technology to be part of how we plan.

💭*Imagine a patient being admitted to the hospital when a nurse asks for their medications and recent test results. Usually, all of this information is stored in the patient's online portal, which they typically access from their phone. However, at this moment, the phone is locked, the password is unavailable, and the recovery number leads to an inactive landline.*

Situations like this are more common than they seem, but they don't have to become roadblocks. What matters is having mechanisms in place to prevent these moments from turning into standstills.

## Device & Digital Identity

Acts as the foundational structure for any life-event planning system. It's a unified digital access point to medical records, financial accounts, legal documents, communication channels, and cloud storage.

### ➢ Review How You Sign In

Open the *Security / Sign-in / Password & Biometrics Settings.* Verify your PIN, password, or, if applicable, fingerprint and face recognition.

### Success looks like:

✅ Device unlocks without repeated errors.

✅ Biometric unlock works on the first or second try.

✅ You aren't relying on a password you haven't tested in months.

### ➢ Check Your Recovery Options

If your recovery info is outdated, password resets may not work as intended. Some services will attempt to verify your identity through prompts on devices or phone numbers you've saved. If these are no longer in use, you won't receive the code necessary to regain access.

You can typically find recovery menus in the following locations:

- Security

- Password & Security
- Login & Security
- Account
- Profile

## What to confirm

✅ **A current phone number** that can receive calls or texts.

✅ **A backup email address** you can retrieve messages from if the primary email isn't operational.

✅ **Any security questions**, if the service supports them.

✅ **Your two-step verification** or **authenticator app options.**

✅ **Any trusted devices** or **backup codes listed** or given by the service.

💡*Note: If you encounter something unfamiliar, click or tap on it. A brief explanation of the item's function will usually appear.*

## ➢ Create a Summary

It gives you and your advocates a clear overview of the devices and accounts that define your digital identity.

## What to list:

- **Main devices** (e.g., "my iPad," "my Samsung phone")
- **Primary email account**
- **Sign-in method,** including PIN, password (not the actual key), or biometric options like fingerprint or facial recognition.

- **Recovery methods** (phone number, backup email, or security questions).

## ➢ Store the Summary Safely

Utilizing both digital and physical versions of your documentation greatly enhances their accessibility and versatility. This dual approach ensures that you have the necessary resources at your fingertips, regardless of the context.

▪ **Capturing digital copies:** use the method most convenient for you, like your mobile device or a printer-scanner. A non-blurry photo of the page counts as one.

▪ **After scanning or photographing the document,** save it to a cloud service you already use—Google Drive, iCloud, OneDrive, or Dropbox.

▪ **Name the file clearly,** for example, *"Account Recovery Outline,"* so it's recognizable months down the road.

▪ **Place a physical copy in a secure, consistent location at home** (e.g., a fireproof safe or a labeled folder) so it's readily accessible.

## ➢ Add a Trusted Recovery Person

While they won't have access to your data, they can assist you in regaining access to your account. The process is generally consistent across various services.

- Open the **Security** or **Recovery** section.

- Find, **Add a trusted contact,** or **Add recovery person.**
- Select a person from your contacts.
- They will get a confirmation message.

## Password & Cloud Management

Without a central system, logins and documents are often scattered across browsers, screenshots, and old devices.

### ➢ Password Managers

Store all your usernames and passwords in a single encrypted vault, accessible with a unique master passphrase. Once you set them up:

▪ **Say goodbye to remembering countless passwords –** the password manager automatically fills them in for you.

▪ **All your devices can be synchronized –** any adjustments you make on your phone are instantly updated on your computer, and vice versa.

▪ **Enjoy automatic backups –** if your devices are lost, stolen, or damaged, your vault remains secure in the cloud.

▪ **Receive security alerts –** you'll be notified if any of your saved passwords are found in known data breaches, allowing you to review them before they can be misused.

### ➢ Set a Strong Passphrase

A passphrase is the main thing users need to remember to access their password manager. To create a secure passphrase, make sure:

- **It is not connected to any personal details.**
- **It is long yet easy for you to recall without writing it down, ideally as a vivid sentence you can visualize.**
  *E.g., "The teapot sings every morning."*

## What to save in a Password Manager

✅Credentials for online accounts, banks, insurance, and utilities

✅Recovery codes for regaining account access if the standard login method is lost

## How to Input Information Into a Password Manager

Once you have your credentials ready to save, you can opt for one of the following methods:

▪ **Import a file:** If your passwords are stored in a browser or on an older device, you can export them to a file in .csv format. This text file lists each record on a separate line, with fields separated by commas.

▪ **Add a new entry:** If your usernames and passwords are written on paper or captured in a screenshot, you can type them in manually.

## ➢ Organize Your Cloud System

Begin by listing all the locations where your files are stored — cloud drives, email attachments, your computer's download folder, or any other place you usually save items.

▪ **If you use multiple services, you may want to simplify your setup.** Some people decide to close accounts they no longer need and centralize their sensitive files in a single primary storage location. Others prefer to keep multiple services but choose one as their main hub.

▪ **Create a clear folder structure that reflects the areas to oversee.** For example, a top-level *"Personal"* folder can include subfolders such as *"Identification"* or *"Care Contacts."*

### How to set up a new folder

👉 **In a cloud's web view:** Select *New* → *Folder*, type the name, and press *Enter.*

👉 **In a mobile app:** Tap the *(+)* or *Create* button, choose *Folder,* enter the name, and save your changes.

### ➢ Implement Cross-Device File Formats

Upload or save files in universally accessible formats that open on any device without special software.

**JPEG/PNG —** best for photos or graphics.

**.docx —** good for documents you update continuously.

**PDFs —** ideal for long-term storage as:

- They preserve the original layout and formatting
- They print cleanly
- They're less likely to be altered by mistake

## How to save your screen content as a PDF

Works with emails, web pages, digital receipts, and forms

### 👉Print → Save as PDF

On laptops or desktops, open the item, select *Print,* then look for *Save as PDF* or *Print to PDF* in the printer list.

### 👉 Share → Save as PDF

On phones and tablets, the *Share* menu includes a *Save as PDF* option. *Useful when you don't see a Print button.*

## How to convert physical documentation to PDF

- Open your phone's *scanning mode*, commonly found in the *Camera, Notes,* or *Files* app.
- Hold the camera over the document. The phone will detect the edges and straighten the image. You can rotate it if needed. If you are not satisfied with the result, tap *Retake*; if you are happy with it, tap *Save.*

## ➢ Configure the Right Access to Your Documentation

By using a cloud service of your choice, you can assign different capabilities to people in your support network.

## Access levels for shared files

- **View Only (or Read Only)**

Users can view and open files, but cannot edit, move, or delete them. This setting is ideal for sharing confidential documents — medical records or financial statements — for review only.

- **Comment/Suggest**

Users can add notes or suggestions without changing the original file. This option is practical when seeking feedback on items like a family budget, a legal draft, or a collaborative project.

- **Edit (or Can Edit / Can Modify)**

Users can open, modify, add, or delete files in the shared folder. This level of access is suitable for caregivers, accountants, or anyone collaborating to keep documents up to date.

- **Full Access / Owner / Co-Owner (varies by service)**

Users have full control over the folder; they can rename, move, adjust sharing permissions, and delete items. This level should be reserved for trusted individuals—a spouse, executor, or long-term support person—who may manage the folder on your behalf.

💡 *Note: Cloud services include a version history feature, which acts as a safety net, allowing you to revert to earlier versions of your document whenever needed.*

Now that you've seen how each permission level determines what others can do with your documents or files, let this be a reminder that early preparation is the backbone of weighing pros and cons in your secure digital planning.

## Health Essentials

When things feel overwhelming, it helps to rely on the applications already tracking your medical history. You don't have to gather everything yourself; instead, focus on understanding what each system records and how it can ease your load and that of anyone supporting you.

### ➢ Patient Portals

**What do they display?** Diagnoses, visit summaries, test results, and upcoming appointments.

**What repetitive tasks can one handle here?** After logging in, look for menus labeled *Appointments, Visits, Schedule,* or *My Care.* This section lets you view your appointments and perform actions such as booking, rescheduling, or canceling.

### ➢ Pharmacy Apps

**What do they display?** Current medications, confirm the addition of new prescriptions, and indicate any discontinued ones.

**What repetitive tasks can one handle here?** After logging in, look for a tab labeled *Medications, Prescriptions, Refills,* or *My Pharmacy.* In this section, you will find options to *Refill, Renew,* or *Order Again* to request your next supply, with pickup or delivery available.

### ➢ Emailed Instructions

To keep track of recent changes in care, such as dosage adjustments, follow-up steps, or new instructions, use the following methods when emails arrive:

- Your email server allows searching messages by keywords: the *physician's name, instructions, visit summary,* or *the email's date.*
- Take advantage of filter categories: *From, Attachments,* or *Unread* to quickly locate important messages.
- Organize health-related emails by creating specific folders or labels to group them.

Because these systems can't be fully integrated due to their distinct databases, objectives, and legal constraints, you can do your best to consolidate the information they produce.

## ➢ Compile a Health Overview

It should bring together timely details for appointments or care coordination. It's not a medical record, but a handy reference.

### What to Include:

✅ **Any new medications**
One line per medication. Add dates if known

✅**Allergies:** What triggers your reactions and how your body responds. (e.g., "Penicillin – rash")

✅A short list of your diagnosed conditions, indicating whether each condition is long-term or newly identified.

✅**Primary Care Provider:** Include the name, phone number, and office address.

✅**Emergency contacts:** List names, relationships, and phone numbers for your emergency contacts.

✅State the name and phone number of your preferred pharmacy. Providing the address is optional unless you have multiple locations.

✅**Insurance Information:** Include your insurance policy number and contact details. It's a good idea to keep a copy of your insurance card with you.

From here, it is sensible to put your preferences and expectations in writing. This includes what matters most to you, how you would like decisions to be handled, and guidance for situations when you cannot be at the center of it all.

## Legal Authority

Legal documents don't override your wishes; they grant the appropriate people the authority to execute them.

- **A Power of Attorney (POA)** designates someone you trust to act on your behalf while you are alive. Depending on the authority you grant, this person can help manage your financial affairs, personal-care decisions, or both.

- **A Will** takes effect only after your lifetime. It outlines how you want your belongings and responsibilities handled, names the people who will receive your assets, and appoints an executor to fulfill your instructions.

- **Advance Directives** focus on your medical care when you cannot speak for yourself. They guide your healthcare team and loved ones by specifying the treatments and comfort measures that reflect your values.

If you're unsure where to begin or want to see the typical structure of these documents, templates can be conducive. They allow you to personalize your plans while maintaining the elements that these documents should contain.

**FreeWill** https://www.freewill.com/
It is an online, user-friendly platform that helps individuals create a basic will or advance directive without requiring any legal background. Through straightforward questionnaires, users are guided step by step, ensuring their wishes are clearly documented and legally recognized.

### ➢ Legal Documents Don't Expire; They Evolve

Even a small change, a new contact, or a revised preference can lead to multiple nearly identical versions of a document.

If someone needs to act quickly, they may not have time to identify which version reflects your true wishes. To avoid confusion, follow these guidelines:

- Retain only the latest signed version in your active folder.
- Move older versions elsewhere or mark them accordingly.
- Use filenames that reflect the document type and year (e.g., "POA_Health_2026.docx")

### ➢ Let People Know What They're Stepping Into

Being named in a legal document is a responsibility, not just a formality. The people you've chosen should:

✅**Know they've been named,** so they're not surprised, and can agree to take on the role, avoiding delay when decisions or actions are time-sensitive.

✅**Understand what they're allowed and expected to do,** so they act within their legal authority and comply with your wishes.

✅**Feel confident about where to find the documents** so they can easily refer to what is needed during an emergency.

## Financial Continuity

It's closely tied to timing and personal responsibility, and it involves taking proactive steps to safeguard your financial well-being, especially during significant life transitions.

▪ **Multi-Recipient Account Alerts** strengthens account oversight by sending notifications to more than one trusted contact. When a bank or investment platform detects unusual activity or significant account changes, these alerts ensure that someone receives the notification promptly and can respond in a timely manner. Examples of events that may trigger alerts include:

- Large withdrawals
- New payees
- Failed login attempts or suspicious transactions
- Low account balances
- Credit card charges
- Changes to contact information

▪ **Automatic Payments and Renewal-tracking** are proactive ways to pay on time, even when someone is ill, overwhelmed, or temporarily unable to manage day-to-day finances. This reduces missed payments, service interruptions, late fees, and lapses in coverage. For caregivers, it reassures that essential services stay active and stable, even if the account holder cannot pay directly.

### ➢ Where it is commonly available:

- Banks and credit unions (bank-level autopay options)
- Utility providers (electricity, water, gas)
- Insurance companies (health, auto, home, life)
- Telecom services (internet, mobile, landline)
- Streaming and subscription platforms

## Caring for Your Digital Life and Legacy

A significant portion of our lives takes place online, resulting in a wealth of valuable digital assets, including photos, messages, and subscriptions. When someone passes away, the platforms that host their data have specific procedures for managing access and transferring that data to loved ones.

### ➢ Apple (iCloud, iPhone, Mac)

**Apple Digital Legacy / Legacy Contact**

Designate one or more “Legacy Contacts” to request access to an Apple account’s data after death, including photos, messages, notes, files, backups, and more. Some items are excluded, such as licensed content and Keychain data like passwords and payment info.

⇢ It applies after Apple receives proof of death and the Legacy Contact's access key, which is provided directly by the person who designates them, either as a QR code or an alphanumeric code.

**If not set up in time:**

✖ iCloud data is heavily protected and usually locked to credentials, with Apple defaulting to keeping accounts private.

✖ Family might face a long, uncertain process needing court orders, and Apple may still not release data or passwords.

✖ Photos, files, and messages can be effectively lost to them, even though they still exist on Apple's servers.

## ➢ Google (Gmail, Drive, Photos, YouTube)

**Google Inactive Account Manager lets users choose:**

- How long the account must be inactive before Google considers it "inactive" (e.g., 3, 6, 12, 18 months).
- Which reliable contacts have access to which services (Gmail, Drive, Photos, etc)
- Whether the account should be deleted after data sharing is complete.

⇢ It applies after a defined period of inactivity. Google detects no sign-in or activity.

**If not set up in time:**

✖ Family members may have difficulty accessing Gmail, as it is regarded as private communication, and email providers enforce strict policies.

✖ Without a password or an Inactive Account Manager, relatives may be able to request account closure, but they will not be able to access the contents meaningfully.

✖ This could result in the inability to retrieve stored documents in Google Drive, photos, receipts, or account-recovery emails for other services.

## ➢ Facebook

**Legacy Contact & Memorialization**

A legacy contact can manage the account after memorialization: write a pinned post, respond to friend requests, change the profile or cover photo, and download shared content if permitted. Similarly, users can choose to permanently delete their accounts once Facebook has completed sharing data that is legally or operationally required.

**If not set up in time:**

✖ Family must separately request memorialization or removal, which may involve submitting proof of death and waiting for review.

✖ No one gets pre-authorized ability to manage tributes, posts, or downloads.

## ➢ Microsoft accounts (Outlook, OneDrive, etc.)

**No “legacy contact”; support-based next-of-kin process**

Microsoft lacks an Apple- or Google-style consumer legacy contact. Families can use support/next-of-kin processes to request account closure or limited data access, which may require legal proof.

⇢ It applies after death if the family initiates a support or legal process.

Family members cannot just "take over" the account. They may be able to request its closure, but accessing meaningful content can be uncertain, as it often depends on jurisdiction and required documentation.

## ➢ Password managers (1Password, LastPass, Bitwarden, etc.)

**Emergency access:** A trusted contact is designated to request access to the vault. There is a set waiting period (e.g., 1–30 days). Once approved, they gain access.

⇢ It applies when the primary account holder is unresponsive (due to incapacity or death).

**Shared vaults:** Users can maintain a shared vault for key logins (banking, utilities, medical portals) that another person already has access to.

**If not set up in time:**

✖ The password manager operates on a zero-knowledge model, meaning the company cannot access user data because it does not know the master password.

✖ Even with a death certificate, families may still struggle to reset the master password.

✖ Because many accounts rely on stored logins, this can effectively prevent families from accessing financial, email, and device accounts unless they have the passwords saved elsewhere.


Connecting Generations
Cyber-Seniors™


be well
ILLINOIS


aetna®


BEYOND
FORCE


trail
TOTAL RETIREE ADVANTAGE ILLINOIS

## DEFINITIONS

***Apple account** is a single set of login credentials, email address, password, and optional security settings that lets you access Apple services such as iCloud, the App Store, iMessage, FaceTime, and device-management features.

***Authenticator app** is a mobile application (e.g., Google Authenticator, Authy, Microsoft Authenticator) that generates time-based one-time passwords or receives push-approval requests.

***Backup** is a copy of data files, system settings, or entire devices stored separately (e.g., on an external drive, cloud service, or another server) so it can be restored if the original is lost, corrupted, or damaged.

- **External drive** is a portable storage device, such as a USB flash drive, external hard disk, or solid-state drive, that connects to a computer via a port (e.g, USB) and provides additional space for saving, backing up, or transferring files outside the computer's internal storage.

***Backup codes** are a set of single-use, randomly generated strings (e.g., 8-digit codes) that you store safely and can enter as the second factor when your primary 2FA method (like an authenticator app or SMS) isn't available.

- **2FA** (two-factor authentication) is a security method that requires two independent proofs of identity before granting access, typically something you know (a password or PIN), something you have (a code from an authenticator app, SMS, or a hardware token), or something you are (a biometric).

***Biometric settings** are the options that control how a device or service uses physical traits, such as fingerprints, facial features, iris patterns, or voice, to verify your identity.

***Browser** is a software program that connects to web servers, downloads web pages, and renders them for you to read and interact with.

***Credentials** are pieces of information, such as a username, email address, password, PIN, or biometric data, that uniquely identify you and prove your authority to access a system, service, or device.

***CSV (Comma-Separated Values)** files are often used to export or import settings, inventory lists, or logs because they can be easily read and edited by spreadsheet programs, scripts, and many operating systems without specialized software.

***Draft** is an unfinished or preliminary version of a document, email, or piece of writing that is saved for later editing and finalization.

***Download folder** is the default location where a device saves files retrieved from the internet.

***Email attachment** is a file, such as a document, image, video, or archive, that is sent along with the body of an email message.

***iCloud data** refers to any files, settings, or information, such as photos, documents, contacts, backups, app data, and keychain entries that are stored on Apple's iCloud cloud service.

***Keychain** is Apple's built-in password-management system that securely stores passwords, credit-card numbers, Wi-Fi credentials, and other sensitive data.

- **Built-in** describes a feature, component, or capability that is included as part of a device, software, or system from the start, requiring no additional installation or external add-on to use.

***Labels (or folders)** in email are organizational tools that let you group messages by topic, sender, project, or any category you choose.

***Login** is the process of entering credentials, such as a username, email, and a secret (password, PIN, biometric scan, or one-time code) to authenticate oneself to a device, application, or online service.

***Mobile app** is a software program designed to run on smartphones or tablets, downloaded from an app store,e and optimized for touch interaction and mobile hardware.

***Passphrase** is a longer, often sentence-like password made up of multiple words, spaces, or characters (e.g., “correct horse battery staple”).

***Password security prompts** (also known as verification or authentication prompts) are a message that the system sends to a secondary device, such as a smartphone, tablet, or another registered computer, to confirm that you are the one trying to log in.

***Scanning mode** on a smartphone is a camera setting that optimizes image capture for reading documents, QR codes, or barcodes.

- **QR code:** (Quick Response code) is a two-dimensional barcode made up of black squares arranged on a white background.

***Screenshot** is a digital image that captures exactly what is displayed on a screen, such as a computer monitor, smartphone, or tablet, at a specific moment, allowing you to save, share, or annotate that visual content.

- **Annotate:** means to add notes, comments, highlights, or other explanatory markings to a document, image, or piece of data.

***Security questions** are personal prompts used as an additional verification method when you create or recover an account. You choose a question (e.g., “What was the name of your first pet?”) and provide an answer that only you should know.

***Sign-in** means proving your identity to a device or online service so that it can recognize you as an authorized user.

***Synchronized** means kept in agreement or updated at the same time across multiple devices, accounts, or systems.

***Tab:** is a selectable element, often displayed as a labeled strip or button, that lets users switch between different sections, pages, or views within the same window or application without opening a new window.

***Two-step verification:** after entering your password, you must provide a second factor, usually a code sent to a phone, a push-notification approval, or a biometric scan, before access is granted.

- **Push-notification:** is a message that a service sends directly to a registered device (phone, tablet, or computer) to alert the user and request an action, such as approving a login, confirming a transaction, or displaying an update, without the user having to open an app first.

***Vault:** is the encrypted container in a password manager that holds all your saved passwords and secure data, unlocked only with your master password.

- **Encrypted** means converting information into a secret code that only someone with the right password or key can read. It keeps the information safe from anyone who shouldn't see it.