Digital Asset Management for a Caregiver

Updated 21-Oct-2021

Introduction

This document provides guidance for partners/caregivers to someone who is approaching end-of-life. It provides an organizational strategy to help you manage *digital assets* that are essential to the logistical tasks that you will face when your loved one is gone. While addressing these items may seem overwhelming now, it becomes much more difficult after your loved one has passed or is no longer able to provide you with the information you will need to manage their digital assets.

My story

My wife Anne was diagnosed with pancreatic cancer in late 2018, and passed away in late 2021. We were supported during Anne's end-of-life by the amazing team at Calvert Hospice.

As an IT professional, I have always nudged family and friends to follow good security practices, and to keep their online accounts and credentials well organized and documented. After Anne died, I realized how often these practices proved valuable in removing barriers during an already difficult time.

I am honored to have this chance to give back to Calvert Hospice by providing this information. I sincerely hope that anyone facing a similar stage in life will find it useful.

What this document is not

This document is strictly focused on accessing and managing your loved one's digital accounts, phone access, etc. It is not meant to serve as legal advice nor does it replace proper estate planning or guidance provided by your hospice caregivers.

What are Digital Assets?

For the purposes of this document, *Digital Assets* refers to online accounts and physical devices that contain or provide access to valuable personal data and/or permit manipulation of those data, authorizing payments, or sending/receiving communication.

Online Accounts

Online accounts are the most common digital asset. Given how many accounts we all use in our daily lives, keeping track of these accounts and their credentials can be difficult. However, it's critical to be aware of what accounts your loved one maintains, and how to access them. Examples include:

- Password Manager account
- Financial accounts
    - Bank, investment, and credit card accounts
    - Employer-based payroll and 401k/403b accounts
    - Tax-related accounts
- Vital online accounts
    - Health insurance accounts
    - MyChart (or parallel) medical care accounts
    - Email/productivity accounts (thru Google, Microsoft, Apple, etc.)
- Other online accounts
    - Social media accounts (Facebook, LinkedIn, etc.)
    - Any other accounts to which your loved one signs in, and to which you would like access after they pass

The best way to ensure you can access these online accounts is to use a *Password Manager* (see the *Password Manager* section below).

Accounts that Can Be Locked

Some accounts may be locked by an institution or company upon their notification of your loved one's passing. This may happen with or without your knowledge, and certainly without your consent. Therefore, it's important to understand under what conditions this might happen.

- Financial accounts in your partner's name only
- Financial accounts for which your partner is the owner, but which manages shared resources
- Financial accounts that manage individual and shared assets
    - In this case, your partner's account may be locked, but yours should remain accessible.
    - You should be aware of any assets that are not jointly held, as your access to those will be gone.
- Other accounts, the content of which you may want to control: Typically, social media accounts like FaceBook and LinkedIn, where you may want to create a legacy page or otherwise preserve the current registration and personal information.
    - FaceBook: (Memorialization Settings -> Your Legacy Contact (https://www.facebook.com/help/103897939701143)
    - LinkedIn:

Smartphone

It's likely your loved one has a smartphone. In today's world, it's important that you can gain access to this device as it may be critical for you to:

- Receive calls and listen to messages
- Send and receive text messages
- Access contacts
- Use the phone for 2-factor authentication as required by any of the accounts above

Make sure you can access your loved one's phone. If they use biometric authentication (finger print, facial recognition), make sure you have configured their phone with your information. Alternatively, make sure you know their PIN or unlock pattern.

Laptop or other devices

It is possible that your loved one will have some other device like a laptop or workstation. Access to this device may serve as a convenience, but could also turn out to be critical depending on what files exist on that device that aren't backed up elsewhere:

- Critical files stored only on this device (medical records, financial information, etc.)
- Personal files such as photos, a diary/journal, or any other content you may want to preserve

Be sure you can access your loved one's laptop or other PC. If they use biometric authentication (finger print, facial recognition), make sure you have configured their device with your information. Alternatively, make sure you know their PIN or password.

Password Manager

Use of a *password manager* is the simplest way to ensure that you and your partner will be able to easily access each other's digital assets should one or the other become incapacitated. Using a password manager, which makes it easy to create and use very secure passwords for all your accounts, coupled with 2-factor authentication on accounts that support it, is the best way to protect yourself online. Setting up a password manager is simple, and provides access to all your accounts in one simple place.

Using a password manager means that you should only ever need to remember one password (to the password manager account); every other password should be stored in this manager, and they should be long, random values that you cannot not remember. (In fact, I even use similar random strings for the answers to security questions. What elementary school did you attend? For me the answer looks like "6u0sC2Lxm!wc7v%c", and it's different for every account!)

How to remember your password manager password?

This is the one password you'll need to remember. We can discuss several strategies for creating a strong password and a reminder.

Password Manager Recommendations

There are lots of lists of the "best" password managers, C|NET is a respected technology resource, and provides this list, which is a good starting point. For dead simple password management, you can use the tools built into your Web browser.

Death Certificate

- Convert to a digital asset
- In today's world, I did not need any hard copies!

Checklist

I am, personally, very list driven. I think it would be very useful to create a list of all the digital assets that you may need access to.

Using the types of accounts listed above, create an entry for each in a table or spreadsheet. Here is a template:

Account	URL	2-factor	Reference	Notes
LastPass	https://www.lastpass.com	- Via phone app	*My* password mgr.	
Wells Fargo	https://www.wellsfargo.com	- Via phone app	Password manager	Joint account, separate logins
TIAA	https://www.tiaa.org	- Text to her phone	Password manager	Her account, lists assets in her name as well as joint assets.

Exercises

All the planning in the world won't prove you can access what you need, when you need it. In the IT profession, it is common practice to perform a test to prove your backup systems and access will work. Why not do the same thing now?

Do a test!

You should do this test:

- Sign in to any account you may need access to without your loved one's help.
    - Use a separate browser profile
    - Focus specifically on accounts that are not joint (see list above)
- Access and navigate through your partner's phone. Make sure you know how to access their email, text messages, and any other 2-factor authentication apps.
- Reboot their laptop, and then be sure you can access it. Browse the file system to be sure you know where any important files are stored.