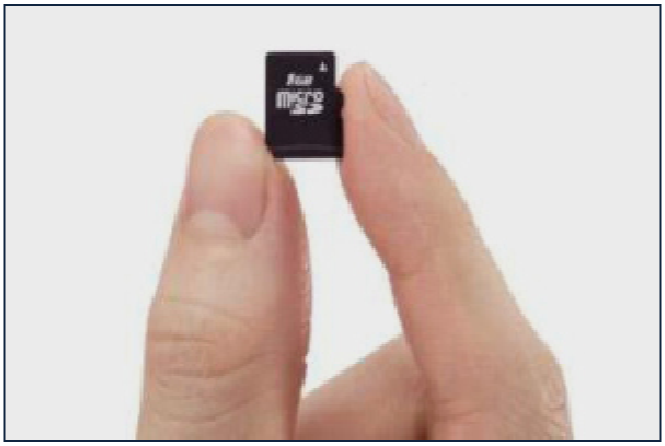
Portable Personal Records for Emergency Situations

By Sig Swanstrom



One aspect of disaster preparation which never seems to get any attention is access to important personal records. These may be urgently needed during a time of disaster or emergency, but without advance planning, you may not have what you need.

Basic records which are critically important, include basic identification such as copies of your driver's license and passport, as well as proof of insurance, basic medical records and copies of prescriptions. You should also have photos of each family member, as well as emergency contact information for family and friends.

Copies of essential records should be kept in three places:

1. Secure protection in your home or place of business;

2. Off-site in a safe deposit box of a financial institution; or, encrypted electronic 'cloud' storage with a company that has its servers in a different state; and

3. An ultra small portable data-storage device which is kept in your wallet, pocket or purse. Since most people are well aware of the needs in the first two categories where there is an abundance of information, this article focuses on the third category which is essential but often overlooked.

A few pages of photocopied documents such as your driver's license, medical cards, and passport, can (and should) be kept in a Ziploc bag stored in your emergency essentials knapsack (Go-Bag). This is a good start, but it isn't nearly enough. Since we live in a data-dependent world, we also need a digital data storage solution which makes it possible to safely carry dozens, or even hundreds of pages, of truly essential records. To do this, we need an ultra-small and durable mobile device, ideally one that is also low cost.

Whatever data is essential to your everyday life and wellbeing, needs to be backed-up and securely stored on a portable device which you keep with you. (Examples of these types of documents are included at the end of this article). Since size and weight are factors which limit practical implementation, this article explains how to responsibly meet this need with minimal inconvenience.

These same documents, and more, should be kept in a safety deposit box or uploaded to cloud storage in a different city or country, but it is still advisable to keep a copy of essential information with you at all times. Disaster often strikes unexpectedly, so access to stored data can be terminally interrupted. For example, if a bank is destroyed in the same storm as your home or place of business, the documents stored at those locations might be gone forever. Similarly, cloud storage of data can be damaged or lost, or it can be inaccessible when you need it.

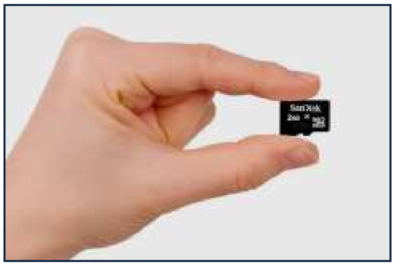
Thankfully, the miniaturization and low-cost of data storage, and advances in data security, now make it possible to carry this essential information with you at all times. Even if your house or office is burned in a fire, damaged as a result of flood or storm, or otherwise inaccessible because you have fled the area to escape from turmoil, or simply because you are on vacation, important records can still be quickly accessible, as long as you have access to a working computer.

This article provides ideas on how you can safely and securely store essential records in a small lightweight package, so that you can keep this important information with you at all times. Various tools can be used to accomplish this, but this article describes what we consider to be the two most viable solutions. The process starts by using a scanner to copy your important records, transforming them into PDF files which can be opened with any computer.

At the end of this article you will find links to free software for making and reading PDF files, and for the products mentioned in this article.

Ultra-Small Data Storage Options

For many, they see their laptop computer or smart phone as the place to store this vital information. That's fine, but since these tools are prone to theft and damage, and security of the data is iffy even if you use security apps, this isn't sufficient. Keeping this data on an encrypted memory card or USB device is far more secure, and even more portable.



Option #1: Memory Card

Memory cards such as those used in digital cameras are relatively inexpensive and ideal for data storage as well as photo storage. Card readers for these memory cards are abundant, but adding an extra small USB card reader to your GO-Bag is nevertheless a good idea. In an emergency situation the data contained on your memory card can be accessed using almost any computer—as long as you have a card reader along.

At little more than ½-inch in size, and less than the weight of two aspirin, the ultra small memory cards like the SanDisk 'micro SD card' (15 mm x 11 mm x 1.0 mm, 0.5 grams), is a portable data marvel. These tiny cards can store from 8GB-32 GB of data or more, so these are ideal for this purpose.

Transport and Packaging of Your Memory Card: After you've added data to your memory card, to protect the card from moisture and damage and still keep the package small, insert the card into a tiny Ziploc bag such as those used for electronic components or jewelry. For added protection, consider adding a piece of rigid plastic to keep the memory card from flexing, and then wrap the bag with a small piece of tinfoil to shield it from static, etc. When you are finished, this little package can still be smaller than ¾-inch (20mm) in size, and less than one gram in weight. Using a piece of duct tape, secure the tiny package to the inside of your wallet for safe storage and ready access, or to the underside of your wristwatch or some other item you wear daily.

Total cost of this project (depending on the storage capacity of the memory card you select), can be as little as $10 (USD). Note: Remember to always encrypt confidential data; see the below section on "Data Security is Essential" for suggestions.

Option #2: 'IronKey' Encrypted Flash Drive

Designed originally for the U.S. government and to meet the needs of those who transport secret corporate data, an IronKey flash drive (aka/ 'USB drive,' or 'thumb drive') is the most secure portable data storage method available to the general public, and it is small enough to carry on your key ring.

An 'IronKey' data storage device requires a password to open it, and the data stored on the drive is fully encrypted. Even the least expensive IronKey model, the D80 (4GB $37; 32GB $116), automatically encrypts anything you add to the drive. Since it uses the high industry standard of 256-bit AES hardware-based encryption, it is very secure. At only 3 x 3/4 x 3/8-inch (75mm x 19mm x 9 mm) in size, and designed to 'plug and play', you can insert it into the USB drive of any computer to quickly access your stored information.

If you want an even higher level of protection, select the IronKey S250 or D250 USB drives (capacities range from 2GB-64GB, $109-599). These have an even higher level of encryption, 256-bit AES Cipher-Block, Chained mode (government-grade) encryption, plus an impressive tamper-proof design of the drive itself. All of the IronKey USB drives are water resistant, but the S250 and D250 drives are waterproof and extra durable.

When kept on your key ring, your IronKey USB device is available for daily tasks such as routine data transfer between computers, as well as for recovery of your personal records after a disaster. Though not as compact as a Micro SD card, the IronKey USB data drive (models S250 or D250) is the option which provides the most durable and secure, portable data storage.

For Info on the D80, Click Here or visit: http://www.ironkey.com/en-US/secure-portable-storage/d80.html

For Info on the S250 and D250, Click Here or visit:http://www.ironkey.com/en-US/secure-portable-storage/250-personal.html

**** If convenience, ease of use, and easy-setup are important to you, a 'IronKey' flash drive is your best choice. If cost or small-size are your most important consideration, then use a Micro SD Card to store your important records.*

Data Security is Essential

If you are storing your data on a memory card or anything other than an IronKey USB drive, confidential data needs to be encrypted. This is essential for keeping your data secure even if your storage device has been lost or stolen. Identity thieves would have a field day if they got their hands on your personal records, so all confidential data needs to be password protected and encrypted before you make it portable.

With both Microsoft and Apple computer operating systems, there is an encryption feature built into the software. Though far from ideal, this software can be used to encrypt the data on a memory card or portable drive. This protection is far better than nothing, but there are better alternatives.

To learn more about the software that is built into your computer's operating system, use the "help" feature of your operating system to learn how to access and use the tool. On PC's running the various versions of Microsoft Windows operating system, the file encryption feature is referred to as 'EFS' (Encrypting File System). If you are using a Mac computer, you will find the encryption software by searching for the term 'FileVault'. Keep in mind that if you utilize either of these methods to encrypt data on your portable drive, you will only be able to access your data by using the same type of computer (PC or Apple), and in some cases, the same version of the operating system. This might seriously limit your ability to access your data after a disastrous event.

To achieve a much higher degree of data security, use the free encryption program, 'TrueCrypt' on your memory card or portable storage device. This free software provides true 256-bit encryption, and it will also run on nearly all desktop and laptop computers. For more information and to download TrueCrypt encryption software, visit: http://www.truecrypt.org/.

TrueCrypt encryption software provides a very high level of encryption, plus it makes it possible to hide encrypted files, so even a hacker who has accessed your memory card won't be able to find the files. On the TrueCrypt website, be sure to read the 'Beginner's Tutorial,' which is part of the TrueCrypt User's Guide. In it you will find instructions on how to set-up the software in '*portable mode*'. This method loads the TrueCrypt encryption software onto the memory card (or flash drive), and lets you partition the drive. This makes it possible for you to run the encryption program on nearly any computer, and lets you store both encrypted and unencrypted data on the same drive. The minimum size for a memory card used for this purpose is 8MB, but a larger memory card will be needed if you plan to store much data.

Whether you use a memory card such as the SD Micro Drive or a flash drive (aka/ 'USB drive,' or 'thumb drive'), remember that you must routinely have it with you, so that your data is available to you when disaster strikes. An encrypted drive that is left behind may not be a security risk, but the work of preparing it will have been wasted if you don't have the drive with you when you need it.

What Records to Store: Encrypted and Unencrypted

Even the most basic personal data such as your driver's license should be encrypted. However, you may want to make some information, such as photos and your address book, accessible without entering a password. At the very least, an unencrypted text file which includes your contact information will make it possible for a lost or stolen drive to be returned to you, and emergency contact information available to authorities, so that they can notify your loved ones if you have been seriously injured.

Remember to add PDF 'reader' software to your memory card or USB device, too. You may need to borrow a computer which does not have this software installed (see links at the end of this article), and the owner of the computer may not want you to download software onto their computer. Or, the Internet may be down making a download impossible.

It's up to you to decide what records you store, and what you encrypt, but don't let a lengthy list delay implementation. It is much better to have an encrypted drive with just a little information stored on it, than to have nothing at all at a time when it's needed.

Start with preparing your memory card or USB drive's encryption. Then, use a scanner to make copies of your most important ID cards and documents, perhaps starting with what you carry in your wallet.

These scanned records should be stored in PDF format, so that your documents can be read, and even printed if necessary, using any computer. The below list isn't *your* list, it's simply included to stimulate your thinking, to help you develop your own list of important documents. If your list is long, don't let the enormity of the task prevent you from starting right now. Store your wallet documents now, and get started with the project today. Continue it as soon as you can.

Consider, too, that you might want to include the same records for your spouse, children, or other close family members or trusted friends. It's a simple task to make two identical sets of emergency records, and two identical portable drives. You might even use the same password on both drives so that you and your spouse can both access either drive.

When you make two identical memory cards or USB drives, your spouse will be able to carry a backup of this same essential information. If you are separated by circumstances, each of you will have what you need. And, if one or the other is lost, damaged or stolen, you will both have what you need on the surviving device.

Records to Consider Including:

1. Driver's License
2. Company or Employee ID
3. Concealed Handgun License (CHL) and Firearm Records
4. Passport (The two page spread which includes your photo)
5. Social Security Card
6. Medical Insurance Cards
7. Dental Insurance Cards

8. Organ Donor Card
9. Pharmaceutical Prescriptions or Prescription Medicine Labels
10. Medical History & Immunization Records
11. Copy of your Last Will and Testament
12. Vehicle Insurance
13. House/Office Insurance Documents
14. Titles for Vehicles and Property
15. Property Descriptions with Serial Numbers
16. Professional Licenses or Certification Documents
17. Credit Card Numbers & Contact Info for Card Companies
18. Banking Information, Including Account Numbers and Passwords
19. List of Other Access Codes and Passwords
20. Important Membership or Affiliation Cards (Particularly those which give you permission to occupy facilities and property which you might want to access during an emergency)
21. Letters of Permission to Occupy Land or Facilities
22. Address Book (Contact information for family, friends and colleagues)
23. Photos (Be sure to include close-up, passport-like images of yourself, family members, key friends and colleagues that you might want to find during an emergency situation.)
24. Physical Description (Yourself, family, friends, and colleagues)
25. Fingerprints and copies of dental x-rays
26. Maps and Directions

Links to Products Mentioned in this Article:

- Free PDF Maker Software: Girdac http://www.girdac.com/Products/PDF-Converters/Free-PDF-Creator/Info/Features.htm

- Free PDF Reader Software:
Adobe http://get.adobe.com/reader/

- Free Encryption Software:
TrueCrypt http://www.truecrypt.org/

- Cloud Storage: 'Dropbox' is one of many options https://www.dropbox.com/

- SanDisk Micro SD Cards, General Information: http://www.sandisk.com/products/memory-cards/microsd/ These cards and card readers are readily available online, as well at electronics stores, and many other retailers such as Costco, Target, and Walmart.

- IronKey D80 Datasheet: http://www.ironkey.com/en-US/resources/documents/Ironkey_D80%20Hardward%20Encrypted%20Flash%20Drive_Sellsheet_Letter.pdf

- IronKey products are *not* readily available from retailers, but they can sometimes be found at online stores such as Amazon.com. The below links are to the IronKey official website:

- IronKey Purchase Info for D80: http://www.ironkey.com/en-US/secure-portable-storage/d80.html

- IronKey S250 and D250 Datasheet: http://www.ironkey.com/en-US/secure-portable-storage/250-personal.html

- IronKey Purchase Info for S250 and D250: http://www.ironkey.com/en-US/secure-portable-storage/250-personal.html

- IronKey Products by Type: http://www.ironkey.com/en-US/resources/documents/IronKey_Product_Diagram_Apr2013.pdf

- IronKey S250 and D250 Comparison Chart: http://www.ironkey.com/en-US/resources/documents/IronKey_S250_vs_D250_SellSheet.pdf

To read other articles on various aspects of preparedness, visit:

www.36ReadyBlog.com