FIPPs

Fair Information Practice Principles

THE GOLD STANDARD FOR PROTECTING PERSONAL INFORMATION

Learning Objectives

- Recognize the Fair Information Practice Principles (FIPPs).
- Demonstrate an understanding of FIPPs by linking principles and practices.
- Accurately apply FIPPs to scenarios involving the collection, use, disclosure, and protection of personal information.

Introduction

Today we purchase just about everything online—clothes, airline tickets, books, to name a few. We use social networks to keep in touch with friends, family, and business associates.

We give companies our credit card numbers to buy goods and services; we share our emails with everyone.

Increasingly, we want to know: How is my information being used? With whom is it being shared? How is it being protected from unauthorized use and disclosure?

A little history…

With the proliferation of computers in the 1970's, organizations began collecting personal information on a grand scale. There were few rules for protecting this electronically captured personal information. In 1974, as part of the Privacy Act, the government defined ***Fair Information Practice Principles (FIPPs*)**. Although these principles are not in themselves law, they form the backbone of privacy law in the United States.

FIPPs today

Since then, FIPPs have become the gold standard for protecting personal information. These tried and true principles provide the terms and conditions by which we collect, use, and retain personal information.

Valuing privacy at Berkeley

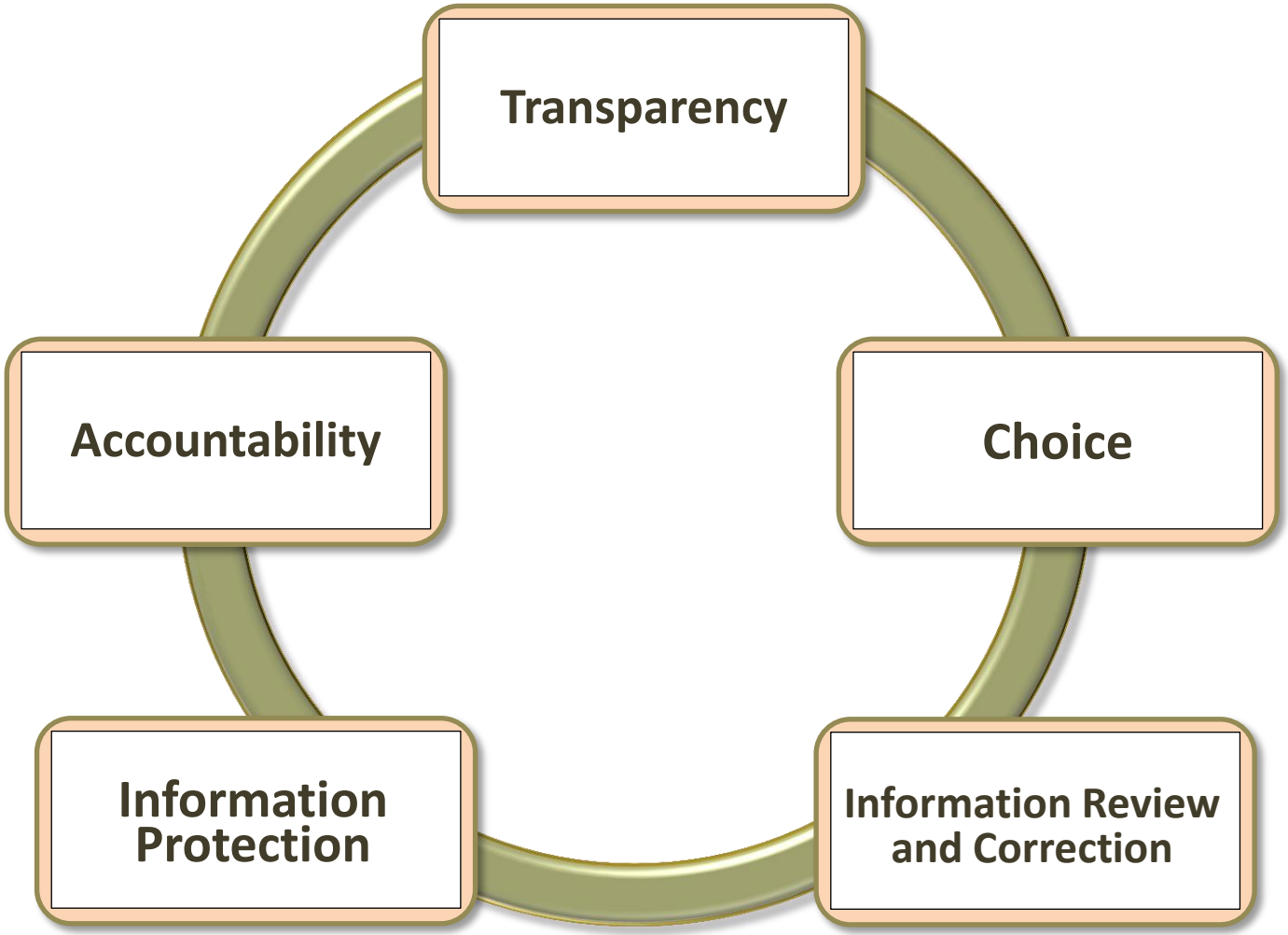
At UC Berkeley, we have a long legacy of protecting the privacy of our students, faculty, and staff. The free flow of information is essential to our mission—to openness and creativity in teaching and research. When personal information is involved, we are responsible for keeping it safe and secure.

Privacy awareness

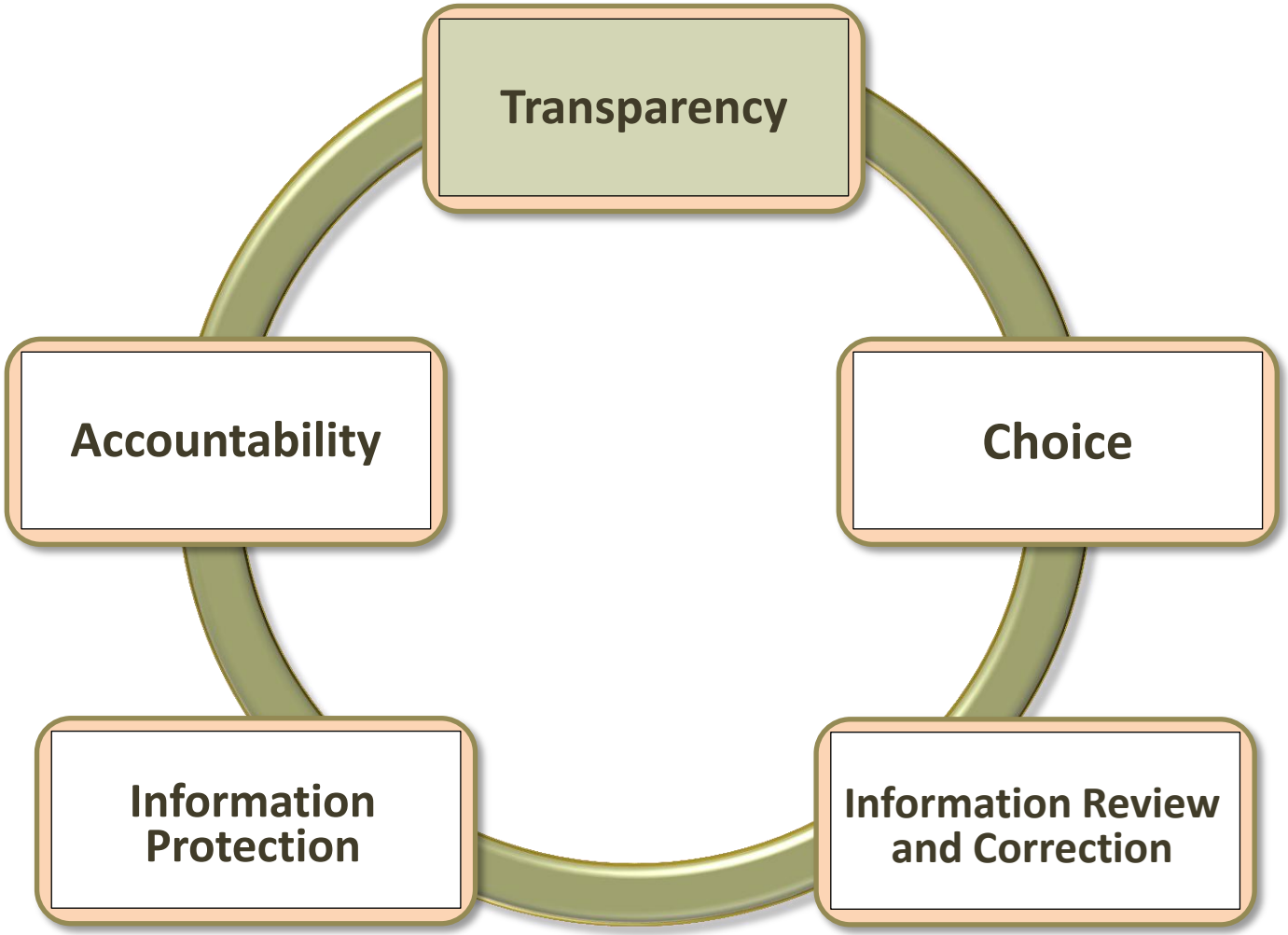
FIPPs guide us to ask questions about how we handle personal information:

- *Has this person been informed about and consented to our privacy practices?*
- *Is this student's personal information properly protected from unauthorized use and disclosure?*
- *Do I need this personal information to do my job?*

The Five Principles



Transparency



Transparency

The Transparency principle promises openness and honesty about the information we collect, use, and retain. In other words, we promise users there will be “no secret data collection”.

Transparency

One way organizations achieve transparency is to disclose their practices in a *Privacy Statement*, which states, for example:

- We will only collect and use your information to complete the following transactions.
- Before we use your information for any other purpose, we will ask your permission.

Transparency

Transparency requires that organizations inform customers about their practices and gain consent *before* collecting or using personal information.

Transparency and Privacy Statements

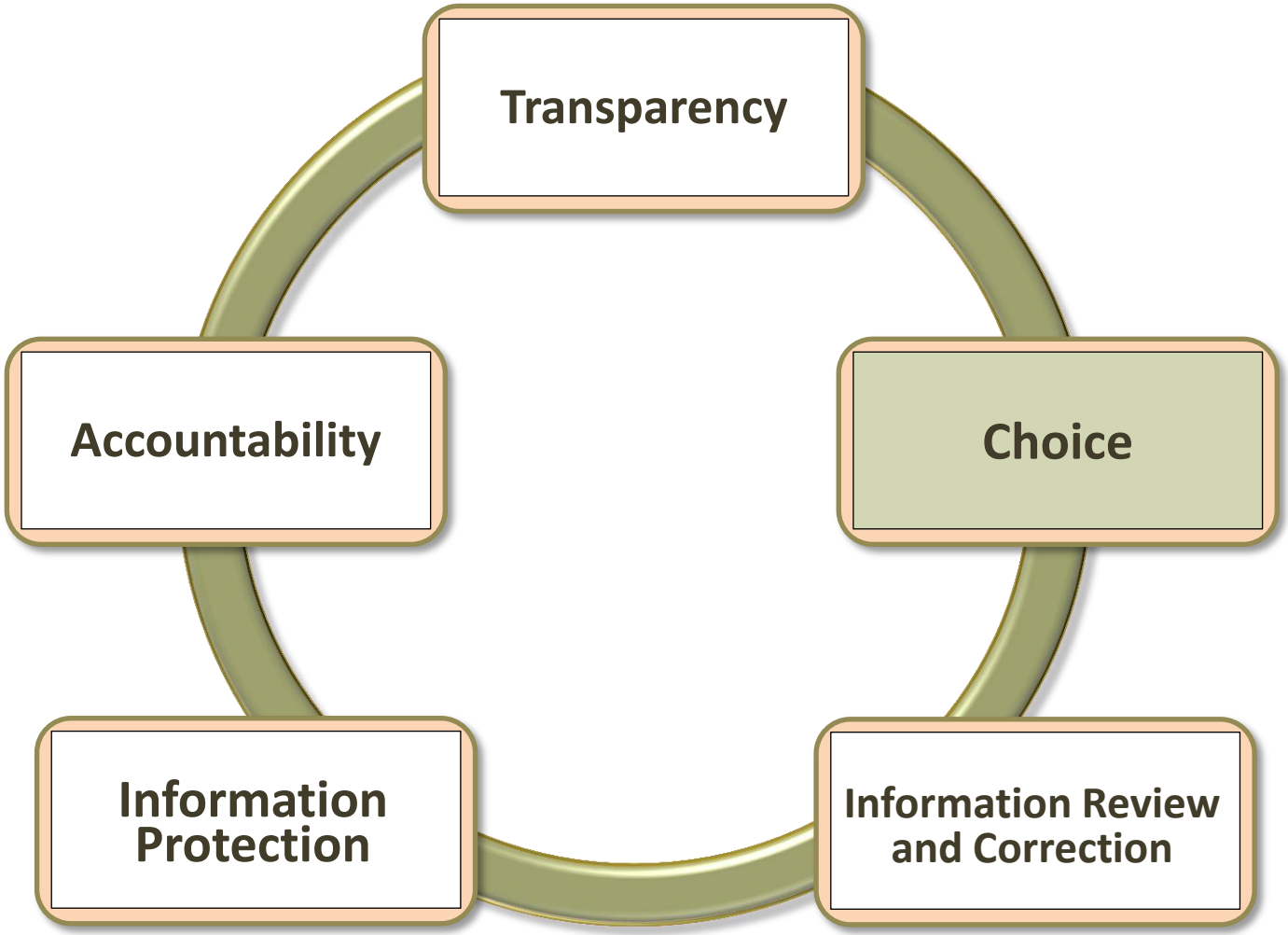
Privacy Statements (including those at Berkeley) are largely based on FIPPs. They outline:

- the purpose of the collection of personal information
- how that information will be used and protected
- whether it will be shared with others; if so, with whom and for what purpose
- how long it will be retained and the manner of disposal

Transparency and Privacy Statements

Privacy Statements should be clearly posted on websites, giving users a *choice* whether or not to disclose personal information.

Choice


Transparency
Choice
Information Review and Correction
Information Protection
Accountability

Choice

Transparency and choice go hand in hand.

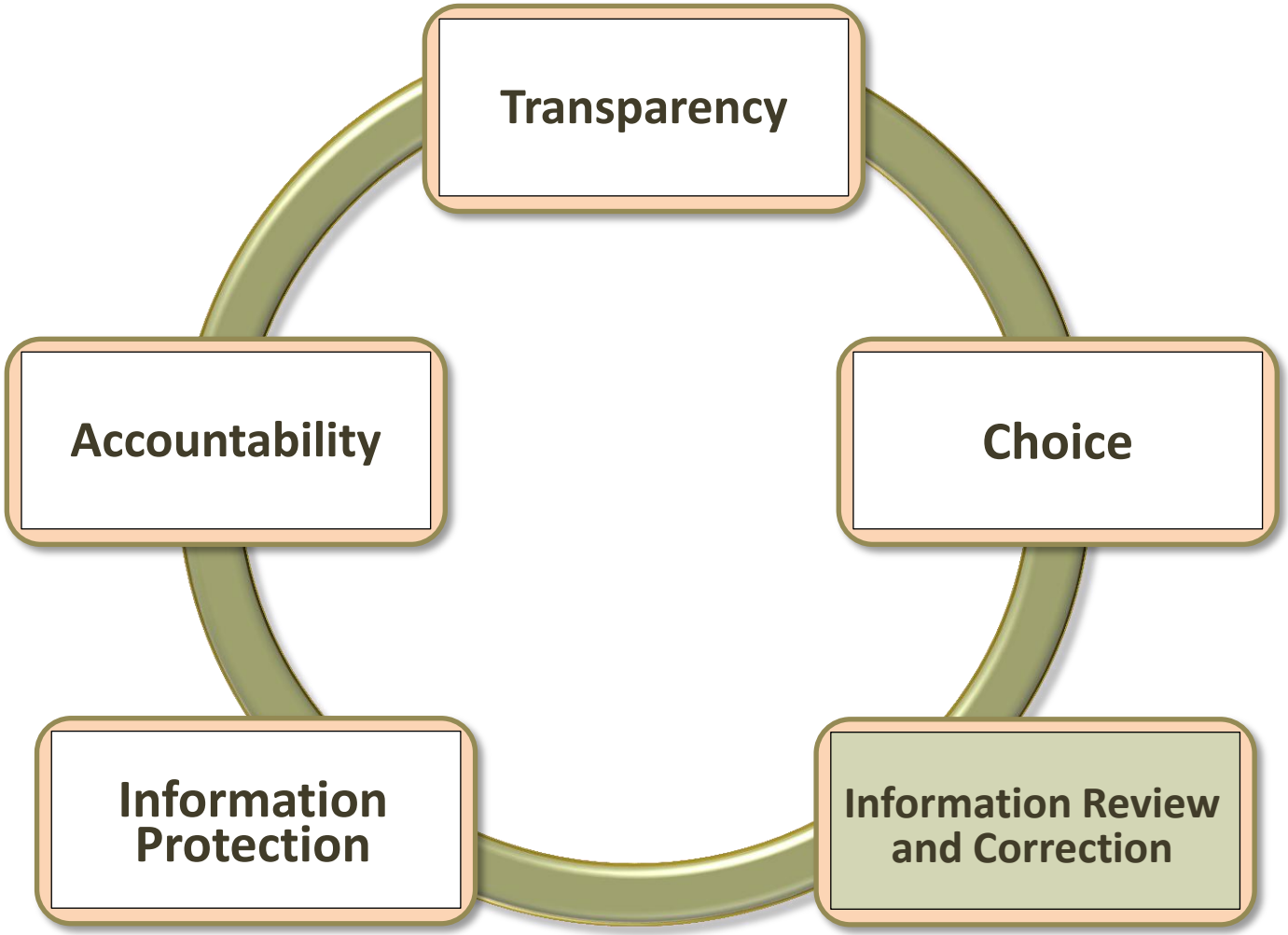
Privacy Statements make privacy practices transparent, giving people the information they need to make informed *choices* about whether or not to disclose personal information.

Choice

Organizations need an individual's consent before collecting personal information. Consent must be for a specific purpose, such as for enrolling a student or for purchasing a book.

If organizations want to use personal information for any other purpose, such as to put people on their mailing lists, they must obtain consent.

Information Review and Correction



Information Review and Correction

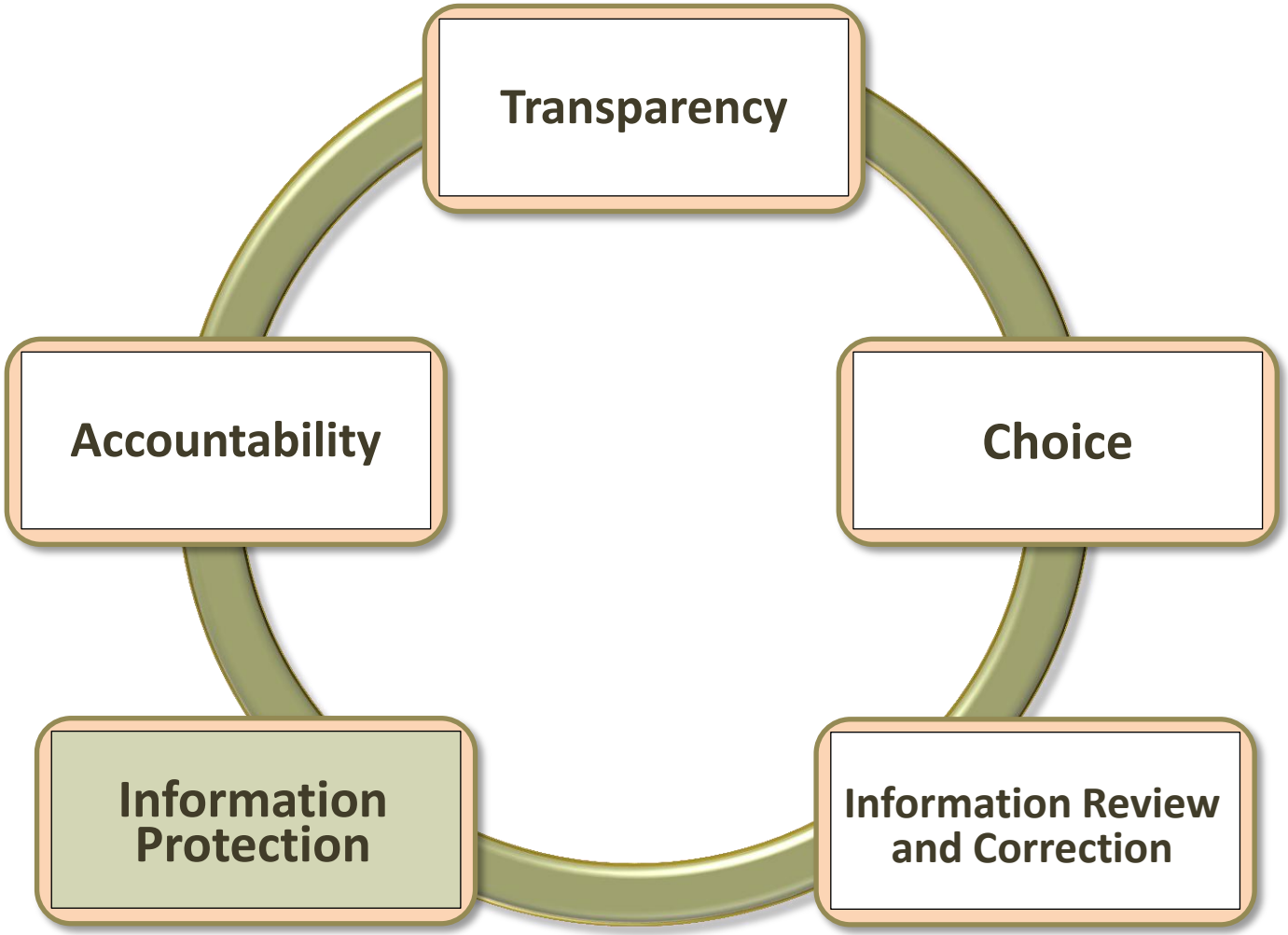
The next FIPPs principle, Information Review and Correction, establishes that individuals should have the right to review and correct personal information.

Information Review and Correction

To ensure data is correct and current, organizations need to provide users access to that information.

If direct access is not possible, then organizations need to provide a means for reporting inaccuracies.

Information Protection



Information Protection

Information Protection ensures that personal information is only used and disclosed under the terms of consent.

In subscribing to this principle, organizations promise to protect the quality and integrity of personal information.

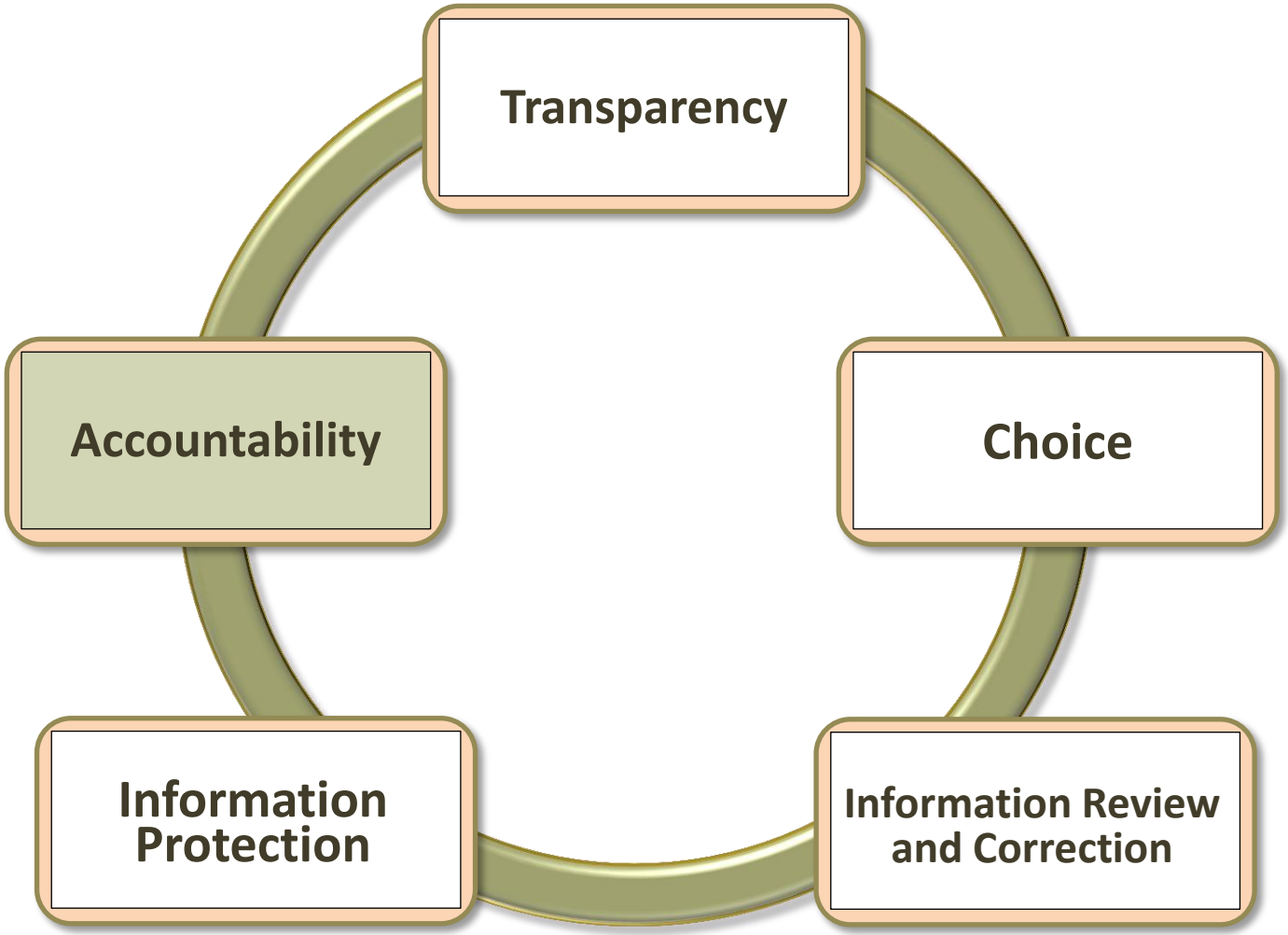
Information Protection

Organizations protect personal information by:

- incorporating FIPPs into their systems and processing
- obtaining information from reputable sources—the best source is always the individual
- only accessing personal information on a "need to know" basis
- conducting regular audits—"scrubbing" files to ensure they are accurate, relevant, and timely

At Berkeley, we conduct "spot check" audits to ensure the quality and integrity of personal data.

Accountability



Accountability

The Accountability principle holds organizations accountable for complying with FIPPs. This training is part of UC Berkeley's ongoing effort to be accountable.

Reporting potential misuses of personal information is another way we hold ourselves accountable. If you suspect that personal protections have been violated, report potential abuses to your supervisor or campus Privacy Officer.

Let's review

- **Transparency**—promises openness and honesty; no secret data collection. One way organizations achieve transparency is to disclose their practices in a *Privacy Statement.*
- **Choice**—gives users a choice whether or not to disclose personal information.
- **Information Review and Correction**—grants users access to their personal information and the opportunity to report anything that they think is incorrect.

Let's review

- **Information Protection**—ensures that personal information is only used and disclosed under the terms of consent. Organizations promise to protect the quality and integrity of personal information.

- **Accountability**—holds organizations accountable for complying with FIPPs. Broadly incorporating FIPPs into campus privacy practices is part of assuming accountability.

Some examples

The following examples illustrate the importance of understanding and applying FIPPs. In some of the following situations, people do the right thing. Others illustrate how a failure to comply with FIPPs can have adverse consequences.

Transparency

Transparency—promises openness and honesty; no secret data collection. One way organizations achieve transparency is to disclose their practices in a *Privacy Statement*.

You have been asked to launch a new website for your unit. You want to adhere to the principle of transparency. In your Privacy Statement, you are specific about what type of information you plan to collect and the purposes for which it will be used and disclosed. But you need to make sure that you have covered all the bases.

Transparency

Refer to the “Privacy Statement for UC Berkeley Websites” policy. At Berkeley, Privacy Statements must adhere to the principles and practices outlined in this policy.

In addition you may want o make sure your supervisor and Privacy Officer review your Privacy Statement. Also ensure that systems and processes have built in proper protections.

Choice

Choice—gives users a choice whether or not to disclose personal information.

David wants to buy a book for a class and finds an online company that offers the best price. He wants to make only this *one* transaction.

The company's Privacy Statement mentions his email address may be added to the company's mailing list in order to be notified of future offers. David knows this will result in a lot of unwanted email. He selects the option "No" when asked if he wants to receive promotional emails.

Choice

Many UC policies and practices are based on choice. For example, a student who doesn't want personal information collected electronically may request another method of collection. Alumni and donors' email addresses may not be added to mail lists without their consent.

Whenever possible, we give the campus community a choice about how their personal information will be used.

Information Review and Correction

Information Review and Correction—grants users access to personal information and the opportunity to report anything they think is incorrect.

Chris has been under treatment at a medical facility. The medical staff have tried several medications to treat him; some were effective, some were not.

He's moving to a new town and wants to make sure all of his records are correct before he moves. He asks to see his medical records and discovers that one of the medications he stopped taking months ago is still listed as current. He requests that his record be updated. Under the FIPPs principle, Information Review and Correction, Chris has the right to access and correct his record.

Information Protection

Information Protection—ensures that personal information is only used and disclosed under the terms of consent. Organizations promise to protect the quality and integrity of personal information.

A man gets a divorce and moves to a new city. He sets up a new email address and bank account. Although he informs the organizations he does business with of these changes, his records are not updated in a timely manner. He discovers his personal information, much of it very sensitive, is still being sent to his ex-wife.

In this example, his personal information has not been properly protected; the quality and integrity of his personal data has been compromised.

Accountability

Accountability—holds organizations accountable for complying with FIPPs.

Berkeley holds itself accountable for complying with FIPPs by broadly incorporating FIPPs into campus privacy practices and daily operations. Our Privacy Office assumes accountability by providing FIPPs training and investigating potential misuses of personal information.

Accountability

Accountability—holds organizations accountable for complying with FIPPs.

Berkeley holds itself accountable for complying with FIPPs by broadly incorporating FIPPs into campus privacy practices and daily operations. Our Privacy Office assumes accountability by providing FIPPs training and investigating potential misuses of personal information.

Summary

FIPPs benefit both organizations and individuals. FIPPs ensure that individuals have choices about how their personal information is used.

Organizations use FIPPs to guide decisions and actions around the collection, use, disclosure, and retention of personal information.

At Berkeley, many of our privacy policies and practices stem from FIPPs.