U.S. FEDERAL TRADE COMMISSION ACT

Section 5: Unfair or Deceptive Acts or Practices (UDAP)

Section 5(a) of the Federal Trade Commission (FTC) Act (15 USC §45) prohibits "unfair or deceptive acts or practices in or affecting commerce." Section 5(b) further empowers the FTC to investigate companies suspected of engaging in unfair or deceptive activities. The FTC also has authority to enforce a variety of sector-specific laws, including the Truth in Lending Act, the Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act, the Children's Online Privacy Protection Act, the Equal Credit Opportunity Act, the Fair Credit Reporting Act, the Fair Debt Collection Practices Act, and the Telemarketing and Consumer Fraud and Abuse Prevention Act. This broad authority allows the FTC to address a wide array of practices affecting consumers, including those emerging with the development of new technologies and business models. Recent cases involving the FTC involve allegations that website operators engaged in deceptive acts by failing to adhere to their own stated policies and practices.

Privacy Policy Considerations

Every privacy policy should be based on the five elements of **notice**, **choice**, **access**, **security** and **redress**. Remember, a privacy policy should be viewed as a binding, enforceable agreement between you and the readers. It should be written clearly and in a language that all readers understand.

A privacy policy should include at least the following information:

1. **Identification of Information Collected**

   A privacy policy should identify the kinds of personal information that is, or will be, collected. This information is commonly referred to as personally identifiable information (PII) and is generally considered "any information that can be used to distinguish or trace an individual's identity" or "any other information that is linked or linkable to an individual." See National Institute of Standards and Technology, "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)," NIST Special Publication 800-122 (2010).

   For instance, the following types of PII may be collected:

   - Name
   - Address
   - Telephone number
   - Email address
   - Credit card information
   - Banking account information
   - Educational information
   - Employment information
   - Personal identification numbers (e.g., Social Security numbers or driver's license numbers)
   - Date of birth
   - Location of birth
   - Biometric records (e.g., photographs, fingerprints, x-rays)

- Protected health information (PHI – medical information related to age, health, prescription medication, or insurance or medical claim-related data)
- Derivative data (typically collected or generated from commercial transactions such as purchase history, customer preferences and geo-locational data)

2. Data Collection and Processing

Is data collected directly from the user or is a third-party source collecting the data and relaying it to you? Will collected data be processed at Duke facilities or will it be processed elsewhere? A statement similar to this will meet the requirements:

> Many Duke.edu websites use Google Analytics (or other similar tools) to collect information about visitor traffic and behavior on our sites. We use these tools to identify usage trends, to improve performance and to enhance website content. We do not use these tools to identify you, and we limit the collection or storage of your personal information.

3. Data Retention

Describe your data retention standards, including how long the data from individuals will be saved.

4. Data Use and Protection

Are there appropriate and reasonable security safeguards in place? If so (the answer should be a resounding yes!), then state this.

5. Data Sharing Intentions

Will data be sent to any business associates or other Duke affiliates for marketing or other purposes? Will data be given or sold to any unrelated third parties and, if so, for what purposes? Describe where and when data will leave Duke.

6. The Individual's Rights and Choices

Does the individual have rights to access, review and make corrections to collected data? Can the individual opt in and/or opt out or otherwise make choices regarding data collection, use and sharing?

7. Children's Privacy

Duke is committed to protecting the privacy of children. If you are not knowingly collecting information from, or targeting your program to, children under the age of 13, say so. Otherwise, the Children's Online Privacy Protection Act (COPPA – 15 U.S.C. § 6502) requires websites and applications (apps) to obtain parental consent before collecting personal information from children under the age of 13.

8. Cookies

Not of the chocolate chip variety! If your site uses cookies or other devices that track site visitors, you must disclose this. Use a statement similar to this:

> Duke websites employ cookies and similar technology to collect aggregate (non-personal) information about your website usage. This allows Duke websites to remember you and to know your preferences when you return to Duke websites. Cookies may remain on your browser unless you delete them or they expire, and some may remain for a period of time while others are erased when you close your browser window. You may adjust your browser settings and decline cookies, but this may impact some features of some Duke websites. To learn more information about cookies and how they work, visit www.allaboutcookies.org.

9. Communications Preferences

Describe if and how the individual can update communication preferences.

10. Contact Information

Provide the name and contact information for the Duke Privacy Program for questions and corrections:

> If you have questions about this privacy statement or any privacy practices at Duke University, please contact privacy@duke.edu.

11. Supplementary Notices and/or Additional Information

If you have additional notices or information for the user, use this area to list and describe this information. Again, a privacy notice should be viewed as a legally binding contract between you and the individual, so you must be transparent with your users.

Legal and Regulatory Considerations

A privacy policy must not only address the kinds of data being processed, but also should consider the legal and regulatory requirements concerning the collection and use of that data. The requirements of a privacy policy should consider the federal and state laws governing the industry to which the company belongs, as well as the laws of the states where its consumers reside.

Specifically, a relevant privacy policy should consider the following federal privacy laws based on the business areas affected:

- **Health Care**
  - The Health Insurance Portability and Accountability Act of 1996 (HIPAA) specifically addresses the privacy of health information. It requires the U.S. Department of Health and Human Services (HHS) to adopt national standards (known as HIPAA Rules) specific to electronic health care information transactions. HIPAA establishes a minimum standard, whereas states are able to develop more rigorous requirements as long as they are in compliance with HIPAA.
  - The Health Information Technology for Economic and Clinical Health Act (HITECH) broadens the scope of privacy and security protections already available under the HIPAA. This law also increases the potential legal liability for noncompliance and provides for more enforcement. HITECH requires data breach notification for unauthorized uses and disclosures of "unsecured (unencrypted) PHI." These breach notification requirements are similar to most state data breach laws relating to PII. For those health providers with an electronic health record (EHR) system in place, patients have a right to access their electronic personal health information (ePHI). Patients can also have their records sent to third parties for a fee that is equal to the labor cost to produce. Additionally, HITECH's enhanced privacy and security standards are applicable to business associates (e.g., accounting firms, billing agencies, law firms) of organizations subject to HIPAA (e.g., health care providers, pharmacies) – including the same civil and criminal penalties – as those HIPAA-regulated organizations with which they work.
- **Business/Workplace**
  - Children's Online Privacy Protection Act (COPPA – 15 U.S.C. § 6502) requires websites and apps to get parental consent before collecting personal information from children under the age of 13. The rule was revised in 2013 to strengthen children's privacy protections and gives parents greater control over the personal information that websites and online services may collect from children under 13.
  - Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM – 16 CFR Part 316) sets the rules for commercial email, establishes requirements for commercial messages, gives recipients the right to stop your emails and spells out severe penalties for violations. The act prohibits false or misleading headers, deceptive subject lines and sending messages to individuals who requested the emails stop. It also requires an opt-out function for future emails and that emails warn when sexually oriented materials are in the messages.

- Telemarketing Sales Rule (16 CFR Part 310) requires telemarketers to make specific disclosures of material information, prohibits misrepresentations, limits the hours that telemarketers may call consumers, and sets payment restrictions for the sale of certain goods and services. The rule's **Do Not Call provisions** prohibit sellers and telemarketers from engaging in certain abusive practices that infringe on consumers' right to be left alone, including calling an individual whose number is listed with the Do Not Call Registry or who has asked not to receive telemarking calls from a particular company. The rule also **prohibits "robocalls"** – prerecorded commercial telemarketing calls to consumers – unless the telemarketers have obtained permission in writing from consumers who want to receive such calls.
- The Health Breach Notification Rule requires certain web-based businesses to notify consumers when the security of their electronic health information is breached.

– **Financial Sector**

- Gramm-Leach-Bliley Act (GLBA) (Public Law 106–102) applies to U.S. financial institutions and protects non-public financial information (e.g., personally identifiable financial information); requires financial institutions – companies that offer consumers financial products or services like loans, financial or investment advice, or insurance – to explain their information-sharing practices to their customers and to safeguard sensitive data.
- Fair Credit Reporting Act of 1970 (FCRA) (15 U.S.C.A. § 1681 et seq.) prevents unreasonable and careless invasions of consumer privacy. The law permits employers, lenders and other persons to obtain copies of individuals' credit reports for legitimate business purposes. However, businesses may not request credit reports unless related to transactions initiated by consumers, such as job interviews or bank loans.
- Fair and Accurate Credit Transactions Act of 2003 (FACTA), which amended the FCRA, requires that companies dispose of credit reports and information derived from them in a safe and secure manner.

– **Education/Student**

- Family Educational Rights and Privacy Act (FERPA) (20 U.S.C.A. § 1232g), protects the privacy of student education records and gives parents the right to examine the scholastic records of their minor children (rights are transferred to the students when they turn 18 or attend college). Additionally, they can correct information in their records that is either inaccurate or misleading. The act broadly defines scholastic records to include all records, files, documents and other materials containing information directly related to students that are maintained by educational agencies or institutions. FERPA permits only certain individuals to have access to student records, including other institution officials who have a legitimate scholastic interest in the records such as teachers, principals and student loan officers. Otherwise, schools must obtain written consent from students or their parents before disclosing any information contained in educational records, although there are a few exceptions (e.g., subpoena request). FERPA applies to all public schools, including colleges and universities, and to private schools that receive federal funding from the U.S. Department of Education.

– **State privacy laws** must also be considered, for example:

- California Online Privacy Protection Act (CalOPPA)
- Delaware Online Privacy and Protection Act (DOPPA)

Mobile Health Applications

Are you developing a mobile health app for use at Duke? You must consider these laws which may apply:

- **Health Insurance Portability and Accountability Act (HIPAA):** The Office for Civil Rights (OCR) within the U.S. Department of Health and Human Services (DHHS) enforces the HIPAA rules, which protect the privacy and security of certain health information and require certain entities to provide notifications of health information breaches.
- **Federal Food, Drug, and Cosmetic Act (FD&C Act):** The U.S. Food and Drug Administration (FDA) enforces this act, which regulates the safety and effectiveness of medical devices, including certain mobile medical apps. The FDA focuses its regulatory oversight on a small subset of health apps that pose a higher risk if they do not work as intended.
- **Federal Trade Commission Act (FTC Act):** The FTC enforces this act, which prohibits deceptive or unfair acts or practices in or affecting commerce, including those relating to privacy and data security, and those involving false or misleading claims about app safety or performance.
- **FTC's Health Breach Notification Rule:** This rule requires certain businesses to provide notifications following breaches of personal health record information. It does not apply to apps created as or on behalf of HIPAA-covered entities, including those acting as HIPAA business associates.
- **FDA's Medical Device Data Systems (MDDS – 21 CFR 880)**: MDDS are hardware or software products that transfer, store, convert formats and display medical device data. MDDS do not modify the data or the display of the data, and do not by themselves control the functions or parameters of any other medical device. MDDS are not intended for active patient monitoring.