LEADERSHIP MESSAGE

As we begin a new decade, it continues to be an exciting time for our organization. At 75-years-old and counting, we’re showing no sign of slowing down. In fact, we’re moving faster than ever, as we lead the charge to reimagine health care.

We continue to grow our GuideWell family of companies to best deliver on our mission to help people and communities achieve better health. Today, more than 13,000 employees serve nearly 27 million people across 34 states, the District of Columbia, Puerto Rico and the U.S. Virgin Islands.

While our commitment to improving access, affordability and quality in health care is what drives us, it’s our commitment to conducting business ethically, with integrity and in compliance with the law, that guides us.

For more than 25 years, our Compass Program has helped shape our organization’s outstanding reputation and allowed us to thrive during decades of change—both at our company and in our industry.

Our commitment to compliance and ethics with our customers, members, stakeholders and the regulatory agencies that govern our business is as important as any other aspect of our business.

We are proud to use our values—respect, integrity, imagination, courage and excellence—in our decision making and firmly believe that we can do well, by doing good. Our outstanding reputation for compliance and ethics provides us with a competitive advantage in the marketplace.

We all have a responsibility to uphold and strengthen that culture. This Compass Code of Ethical Business Conduct explains our responsibilities for conducting business ethically. We encourage you to read this information and use it as a valuable resource in your day-to-day business activities.

Your support and commitment to compliance will help ensure many more years of success in helping people and communities achieve better health.

Cordially,

CEO

Chair, Audit & Compliance Committee

VP, Chief Integrity & Compliance Officer
GuideWell Mutual Holding Corporation is the parent organization to a family of companies focused on transforming health care and offering a broad range of health-related products and services. Through a portfolio of forward-thinking companies and partnerships, from start-ups to industry leaders, we embrace emerging technologies and drive market innovations designed to improve the health care system and help people take an active role in their health. These companies include:

- Our health insurance business, which provides innovative health solutions and insurance plans to the people of Florida. We have served Floridians since 1944, offering an array of health and wellness products and services to fit the individual needs of those we serve;
- GuideWell Health, focused on delivering superior health outcomes and experiences to patients through new, innovative care delivery models;
- GuideWell Connect (including Onlife Health), our consumer and retail services business, which helps clients connect with their customers and provides them with the support they need;
- GuideWell Source, the parent company of First Coast Service Options and Novitas Solutions, which provide administrative and claims processing services for state and federal health care programs such as Medicare and Medicaid; and
- PopHealthCare, the GuideWell subsidiary that provides services to many health plans and is supported by GuideWell’s expertise, resources and relationships.

Our GuideWell family of companies is guided by the same mission, vision and values.

**MISSION**
To help people and communities achieve better health

**VISION**
A leading innovator enabling healthy communities

**VALUES**
The beliefs and priorities that drive our company’s culture are our values of respect, integrity, imagination, courage and excellence
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Integrity and Ethics</strong></td>
<td>6</td>
</tr>
<tr>
<td>Our Commitment</td>
<td>7</td>
</tr>
<tr>
<td>Compass Program</td>
<td>7</td>
</tr>
<tr>
<td>Code of Ethical Business Conduct</td>
<td>7</td>
</tr>
<tr>
<td>Disciplinary Action</td>
<td>8</td>
</tr>
<tr>
<td>Why Ethics, Integrity and Compliance Count</td>
<td>9</td>
</tr>
<tr>
<td>Our Ethical Decision-making Framework</td>
<td>10</td>
</tr>
<tr>
<td><strong>Our Responsibility and Reporting Concerns</strong></td>
<td>12</td>
</tr>
<tr>
<td>Management and Individual Responsibility</td>
<td>13</td>
</tr>
<tr>
<td>Providing Ways to Report Situations Without Fear of Reprisal</td>
<td>13</td>
</tr>
<tr>
<td>Keeping it Confidential</td>
<td>14</td>
</tr>
<tr>
<td>We Will Not Tolerate Retaliation</td>
<td>15</td>
</tr>
<tr>
<td><strong>Our Environment</strong></td>
<td>16</td>
</tr>
<tr>
<td>Creating a Professional Environment</td>
<td>17</td>
</tr>
<tr>
<td>Maintaining a Safe Work Environment</td>
<td>17</td>
</tr>
<tr>
<td>Discriminatory and Sexual Harassment</td>
<td>18</td>
</tr>
<tr>
<td>Equal Employment Opportunities</td>
<td>19</td>
</tr>
<tr>
<td>Soliciting and Distributing Literature</td>
<td>20</td>
</tr>
<tr>
<td><strong>Dealing with the Marketplace and Business Partners</strong></td>
<td>22</td>
</tr>
<tr>
<td>Fair Competition and Business Ventures</td>
<td>23</td>
</tr>
<tr>
<td>Advertising and Marketing</td>
<td>25</td>
</tr>
<tr>
<td><strong>Use of Company Assets</strong></td>
<td>27</td>
</tr>
<tr>
<td>Using Company Assets</td>
<td>28</td>
</tr>
<tr>
<td>Using the Internet, Email and Social Media</td>
<td>29</td>
</tr>
<tr>
<td>Procurement of Goods and Services</td>
<td>31</td>
</tr>
<tr>
<td><strong>Conflicts of Interest</strong></td>
<td>34</td>
</tr>
<tr>
<td>Conflicts of Interest</td>
<td>35</td>
</tr>
</tbody>
</table>
Gifts and Entertainment
Gifts and Entertainment
Charitable Giving and Community Investment
Accurate Company Records and Financial Integrity
Accurate Record Keeping
Travel
Protecting Information and Property
Privacy
Confidential, Proprietary and Other Non-public Information
Employee Data and Verification of Employment
Retention of Records
Copyrights
International Travel Restrictions
Protecting our Brands
Information Security
Information Security
Dealings with Government Programs and Interactions with the Public
Working with Government Customers
Political Contributions and Lobbying Activities
Activities Abroad
Legal and Regulatory Requirements
Legal and Regulatory Requirements
INTEGRITY AND ETHICS

- Our Commitment
- Compass Program
- Code of Ethical Business Conduct
- Disciplinary Action
- Why Ethics, Integrity and Compliance Count
- Our Ethical Decision-making Framework
OUR COMMITMENT

We have a deep commitment to conducting business ethically, with integrity and in compliance with the law.

Our compliance vision is to advance a corporate culture, guided by the highest standards of integrity and ethical business conduct, that demonstrates our deep commitment to compliance with all applicable laws and regulations. Strengthening our commitment to compliance not only reinforces our mission and our values but also provides us with a competitive advantage in the marketplace.

COMPASS PROGRAM

The Compass Program serves as our compliance and ethics program. The program is designed to educate all company board members, officers, employees, temporary workers, contractors, and representatives of the company* on ethical behavior in the workplace. It also provides an avenue for employees to get answers to compliance and ethics questions and report suspected misconduct.

CODE OF ETHICAL BUSINESS CONDUCT

This booklet is our official Code of Ethical Business Conduct (“Compass Code of Conduct”), an important part of the Compass Program. It provides guidance on

*All referred to as “employees” in this booklet.

Here is how you can help us live up to that commitment every day.
You are required to read, understand and comply with the Compass Code of Conduct, in addition to complying with all company policies and procedures.

applying the company’s commitment to integrity and ethical business conduct to day-to-day business situations and activities. The Compass Code of Conduct supplements company policies and procedures, which provide more detailed guidance on company expectations and requirements for behavior in the workplace and while conducting company business.

The Compass Code of Conduct applies to Guidewell Mutual Holding Corporation, certain subsidiaries and affiliates, and employees of the company. GuideWell Mutual Holding Corporation and certain subsidiaries and affiliates are collectively referred to as the “company.”

The Compass Code of Conduct and company policies and procedures are located on the company’s intranet home page. The Compass Code of Conduct can also be found at www.floridablue.com by clicking About Us and then by clicking the Ethics & Compliance section.

DISCIPLINARY ACTION

Disciplinary action, including termination of employment and legal action, may result in response to violations of law, company policy or the Compass Code of Conduct, or in cases of other misconduct or unethical behavior.

The types of misconduct that are likely to result in disciplinary action include, but are not limited to:

- Violating or directing others to violate the law or company policies;
- Failing to promptly raise a concern regarding illegal or unethical activity;
- Failing to cooperate with investigations into compliance allegations;
WHY ETHICS, INTEGRITY AND COMPLIANCE COUNT

Acting ethically, with the highest integrity and in compliance with the law, is as important as any aspect of our business. How you conduct yourself reflects on you and the company.

That is why we expect and require that you comply with all applicable laws and regulations in carrying out your responsibilities. Laws do not cover all situations, and sometimes laws permit actions that do not promote the level of honesty, fairness or integrity the company expects.

We expect you will:

- Promote the safety and welfare of employees and our customers
- Encourage a cooperative and professional work environment
- Protect personal rights and corporate property
- Demonstrate the highest standard of integrity and ethical behavior

Retaliation is any adverse action taken against an individual for filing, in good faith, a report or inquiry or participating in an investigation of a report or inquiry.

- Retaliating against an employee who has made a good faith report of potential violations or who has cooperated in a compliance investigation; and/or
- Making an allegation in bad faith and/or other intentionally false allegations of misconduct.
OUR ETHICAL DECISION-MAKING FRAMEWORK

When faced with an ethics issue or concern, the best course of action is not always clear.

The ethical decision-making process is a series of questions that you should ask yourself anytime you are not sure about what you should do in a particular situation. This is especially important if there is something about the situation which makes you question whether what you are about to do, or what you are being asked to do, is right or wrong.

To help guide you on your course through ethical decision-making, consider the following questions when you are unsure whether an action or situation is appropriate.

**Gain Clarity**

- What feels wrong about the situation?
- Can you identify the ethics issue involved?
- Does this situation conflict with our values?

*Identify and clarify the ethics issue at stake in a situation when you are unsure.*
- Consult Resources
  - Does anything about this situation violate our Compass Program, company policy or the law?
  - Consult our company resources to determine whether a situation goes against our Compass Program, company policy or the law.

- Consider the Consequences
  - How will our customers or others be affected by my decision?
  - What effect could this decision have on the company’s reputation and on my own?
  - Focus on the effect your decision will have on our customers and fellow employees. Who has an interest at stake? Who will be helped or hurt by your decision? Would you want to read about this in the news?
OUR RESPONSIBILITY AND REPORTING CONCERNS

- Management and Individual Responsibility
- Providing Ways to Report Situations Without Fear of Retaliation
- Keeping it Confidential
- We Will Not Tolerate Retaliation
MANAGEMENT AND INDIVIDUAL RESPONSIBILITY

You have the right and the responsibility to question or challenge situations you suspect are unethical or violate company policies, the Compass Code of Conduct, or any law or regulation.

By raising your concerns, you are helping to protect yourself, your colleagues, our company, our employees, and our customers. You should raise concerns or seek guidance if you are unsure or have an uneasy feeling about whether certain behaviors or activities are consistent with standards of ethical business conduct. We do not expect every employee to have the answer to every ethical question, but we do expect every employee to know when to ask for help and where to go for help.

All levels of management should clearly articulate our commitment to compliance and create an open environment where employees can report unethical or compliance situations, without fear of retaliation or reprisal. If a compliance-related question or concern is received, it should be addressed promptly and management should engage the appropriate parties (e.g., Compass, Employee Relations, Legal Affairs) who can work toward a resolution, all while keeping confidentiality to the extent possible.

PROVIDING WAYS TO REPORT SITUATIONS WITHOUT FEAR OF REPRISAL

You should first discuss the situation with your immediate supervisor.

Give your supervisor the opportunity to address the situation. If the situation is not handled
to your satisfaction, or you are not comfortable talking to your supervisor, we provide many additional ways to make an inquiry or report a situation without fear of reprisal.

You may contact the Compass Helpline at 1-800-477-3736 x56300 at any time or access the EthicsPoint website at www.compass.ethicspoint.com. Both avenues give you the option of making an inquiry or reporting a situation without disclosing your identity.

If you prefer, you may contact Business Ethics, Integrity & Compliance directly: Colleen Brennan, Vice President and Chief Integrity and Compliance Officer (904) 905-5068 x55068 or Tammy Holton, Senior Manager, Business Ethics (904) 905-4264 x54264. You may also contact Legal Affairs at (904) 905-8720 x58720 or Employee Relations at (904) 905-4995 x54995. We are here to help.

---

**KEEPING IT CONFIDENTIAL**

Our company has partnered with EthicsPoint, an outside vendor that provides a 24/7 service via the telephone or by website. This allows individuals the ability to either talk to a compliance representative or go directly to the EthicsPoint website to ask a question or file a report. Our vendor also allows you to receive an up-to-date status on any report you file.

A report key will be provided to you at the time you ask a question or file a report. We will use the report key to communicate with you and ask follow-up questions, when necessary. You can log on to EthicsPoint at any time, enter your report key and receive an update on your report. We will protect your confidentiality, although sometimes it is difficult to investigate situations without involving you, so we may ask you if you are willing to identify yourself. We believe it is better for you to come forward than to let the situation continue. Our company has a non-retaliation policy to protect you.
If you choose to make an anonymous report, you should provide enough information about the situation to allow us to properly investigate it. It can hamper our investigation if we do not have enough information.

**Information needed when you make a report:**

- Describe the situation in detail and include the business area and people involved.
- Identify dates when events occurred.
- Let us know if you observed the activity directly or someone told you about it.
- Tell us how the situation occurred (e.g., Was the procedure not followed? Was someone told to do something inappropriate?).
- Describe any relevant documents that could help us investigate the matter.

**WE WILL NOT TOLERATE RETALIATION**

**Reporting activities that violate our Compass Code of Conduct is vital to maintaining a strong culture of compliance.**

We protect employees who, in good-faith, report wrongdoing or unethical behavior by prohibiting retaliation. It is a violation of the Compass Code of Conduct and considered misconduct to retaliate against an employee for reporting an ethical or legal concern, in good faith. We expect management to create an open environment for employees to report issues, regardless of what the outcome may be. Retaliation for good faith reports will result in disciplinary action up to and including termination and, in some cases, retaliation is also against the law. If you suspect that you or someone you know has been retaliated against for raising a concern, immediately contact Compass, Legal Affairs or an Employee Relations consultant.
3
OUR ENVIRONMENT

- Creating a Professional Environment
- Maintaining a Safe Work Environment
- Discriminatory and Sexual Harassment
- Equal Employment Opportunities
- Soliciting and Distributing Literature
CREATING A PROFESSIONAL ENVIRONMENT

All employees are expected to conduct themselves in a manner that promotes the safety and welfare of employees; encourages a cooperative, courteous and productive environment; and protects personal rights and corporate property.

Each of us needs to treat our fellow employees, customers and the public with respect and dignity, and hold ourselves accountable for our actions and behavior. Any form of harassment (sexual or otherwise), intimidation (e.g., bullying) or retaliation will not be tolerated by our company.

MAINTAINING A SAFE WORK ENVIRONMENT

We are committed to maintaining a safe and healthy workplace that is free from hazards and promotes a productive working environment.

Here are some basics to remember:

- Abide by the terms of our company’s drug-free workplace policy as a condition of continued employment.
- No weapons of any type are permitted to be carried in a company office at any time except by law enforcement officers and company security officers who have been authorized by the company to do so.
• Report convictions, indictments, charges, and updated court dispositions of any criminal misdemeanor or felony to Employee Relations.
• Comply with all laws and regulations affecting safety, health and environmental protection.
• Comply with our fire, safety, health and security policies and procedures.
• Notify your management if you perceive conditions to be unsafe, unhealthy or hazardous to the environment.

**DISCRIMINATORY AND SEXUAL HARASSMENT**

Discriminatory harassment is misconduct based on race, color, religion, national origin, disability, sex, age, gender identity or expression, sexual orientation, veteran status or marital status.

Sexual harassment is a specific form of sex discrimination. It includes any unwelcome sexual advances, requests for sexual favors, and other verbal, physical, or written conduct of a sexual nature in any of three situations:

• When submission to conduct is made either explicitly or implicitly a term or condition of an individual’s employment;
• When submission to or rejection of conduct by an individual is used as a basis for employment decisions affecting such individual; or
• When conduct has the purpose or effect of unreasonably interfering with an individual’s work performance or creating an intimidating, hostile or offensive working environment.

*We prohibit and will not tolerate discriminatory or sexual harassment. Any such conduct may result in disciplinary action up to and including termination of employment.*
Here are some basics to remember:

- Treat fellow employees, customers and the public with professionalism, respect and dignity at all times.
- Report and constructively confront all incidents of harassment.
- Retaliation against employees for reporting harassment, or assisting in an investigation, will not be tolerated and may result in disciplinary action up to and including termination of employment.
- Do not engage in any form of harassment including any based on race, color, religion, national origin, disability, sex, age, gender identity or expression, sexual orientation, veteran status or marital status.

EQUAL EMPLOYMENT OPPORTUNITIES

Our policy is that applicants will be recruited, selected, hired and promoted based on their individual merit and ability.

Our continued success depends on the strength and abilities of our employees, regardless of race, color, religion, national origin, disability, sex, age, gender identity or expression, sexual orientation, veteran status or marital status. We support equal employment opportunity principles and promote diversity in our workforce, and we are committed, through our affinity based groups, now known as GuideWell Communities, and affirmative action program, to employ, promote and treat employees according to their ability and without discrimination.
Here are some basics to remember:

- All employment decisions and practices are based on job performance, experience and qualifications. This includes recruitment, hiring, training, development, compensation, benefits, promotions, transfers, corrective action, corporate-sponsored educational, social and recreational programs and terminations.

- All members of management are accountable for supporting our Equal Employment Opportunity policy and affirmative action program.

- The company will not tolerate any employment-related discriminatory practices.

SOLICITING AND DISTRIBUTING LITERATURE

To prevent disruption of business activities, minimize distractions for all employees, and preserve company security and confidentiality, solicitation of funds by employees during work time is prohibited. Distribution of literature by employees during work time or in work areas is also prohibited.

Here are some basics to remember:

- Soliciting and distributing literature by non-employees on company property or using company assets is prohibited at all times.

- Do not distribute literature in work areas or during work time.

- Get approval from Corporate Social Responsibility before soliciting for charitable contributions.
Q: Our team would like to participate in a college basketball tournament office betting pool. Is this allowed?  
A: No. Our Compass Program and our policies prohibit gambling in the workplace.

Q: My son's baseball team is selling cookies as a fundraiser for his school. Is it OK for me to sell cookies at work?  
A: No. Selling any item during work time and/or in work areas is not allowed.

Q: My wife has a new hair salon that she is trying to promote. She gave me fliers to post on the bulletin board in the break room. Can I do this?  
A: No. Distribution of literature is not allowed.
DEALING WITH THE MARKETPLACE AND BUSINESS PARTNERS

- Fair Competition and Business Ventures
- Advertising and Marketing
FAIR COMPETITION AND BUSINESS VENTURES

We are committed to fair competition and do not engage in practices that illegally restrain trade or reduce competition.

Our business activities must comply with federal and state antitrust laws that encourage competition and prohibit certain activities limiting competition. Additionally, many of the activities that violate federal or state antitrust laws may also violate federal and state unfair trade practice, trade secret, and procurement laws and regulations. Some examples of practices and agreements that are considered unlawful activities in restraint of trade include price fixing, bid collusion, allocating or dividing customers or markets, and agreements to boycott or refuse to deal with competitors, customers or suppliers.

Another unlawful practice is the use of market power to unfairly or unreasonably exclude competitors or suppliers, or to influence product or service tie-ins where the availability of one product or service to a customer is conditioned upon the purchase of another.

Q: My friend works for a competitor and our conversation over dinner turned work-related. He began to ask questions about our company’s market strategy and pricing. Since I’m not at work can I discuss this information?

A: No. You should avoid discussions with current or potential competitors on topics such as this, whether at work, in social settings, or at trade/professional association meetings.
Here are some basics to remember:

- Set pricing for products and services independently, and not in consultation with any other potential provider of those products or services.

- Avoid discussing or otherwise sharing pricing information with individuals who do not work for the company, especially at trade or professional meetings or events that our competitors may attend. If such a discussion begins, and regardless of the setting, excuse yourself immediately. An unlawful agreement involving us may end up being implied by your attendance at such discussions even if you do not participate in them.

- Avoid discussing the company’s business relationships with vendors or customers with anyone uninvolved in those relationships.

- Clear all agreements involving exclusive relationships, preferential pricing terms or commitments not to deal with others through Legal Affairs.

- Coordinate all merger and acquisition, joint venture and teaming arrangement discussions and agreements through Legal Affairs as early as possible.

Here are some situations to always avoid:

- Agreements with one business or individual that limit the company’s ability to seek the most competitive terms possible with another business or individual.

- Formal or informal alliances with health care providers or others that seek to insulate the company or others from competition.

- “Take it or leave it” contractual terms imposed on others.

- Any statements, whether written or not, to competitors or others that could be understood to be an agreement to set prices, collude or engage in some other non-competitive arrangement.
ADVERTISING AND MARKETING

Our advertising, including written marketing materials and oral representations by employees, agents, or business partners, should always be clear, complete and accurate.

Enterprise Marketing must review all of our advertising. Additionally, there are special rules that apply to certain state and federal lines of business (e.g., Medicare) with which you should be familiar.

Here are some basics to remember:

- Do not make misrepresentations or misleading statements to anyone. If you make specific claims about the company’s benefit plans, products or services, you must have a good faith basis for those claims.

- Plans, products or services should not be marketed in any way that might cause

Q: At a meeting of my professional association, some of the members talked about a plan to divide their sales territories to reduce competition. I did not agree to participate, but what should I say if this happens again?

A: Collusion is a serious violation of law. Anytime you are in a meeting with competitors and the discussion turns to topics that could be or are anticompetitive, you should excuse yourself from the meeting and contact Legal Affairs or Compass as soon as possible.
confusion between our plans, products or services and those of competitors. If you believe a customer or potential customer may have misunderstood you, promptly correct any misunderstanding.

- You should be alert to any situation where a competitor may attempt to mislead potential customers and inform your immediate manager or Legal Affairs of these situations.
- Do not disparage any of the products, services or employees of any competitor.
USE OF COMPANY ASSETS

- Using Company Assets
- Using the Internet, Email and Social Media
- Procurement of Goods and Services
USING COMPANY ASSETS
You are responsible for ensuring that company assets are used responsibly.

Company assets include both tangible and intangible property ranging from computers, office equipment, Wi-Fi, furniture and supplies to intellectual property, data, strategies and financial and other business and customer information. The theft, misappropriation or unauthorized copying, storage, sale, destruction or modification of company assets is misconduct that may result in disciplinary or legal action against you.

Here are some basics to remember:

- Do not use company assets for personal gain.
- Do not transfer any company assets to other people or entities, unless it is required in the ordinary course of business, and the appropriate safeguards (e.g., contracts) are in place.
- Do not extend credit to any board member or employee (other than assisting with authorized relocation expenses or emergency disaster relief efforts).
- Report incidences of lost, damaged or stolen assets to your management, the Safety and Security department, or Compass.

Examples of intellectual property include, but are not limited to, information security architecture, application source code, programs, and prototypes.
USING THE INTERNET, EMAIL AND SOCIAL MEDIA

The company provides information technology resources including Internet and email for business purposes. The company allows professional and limited personal use of information technology resources, including social media, for occasional, brief activities which do not interfere with job responsibilities or violate the law or any company policy.

We monitor email and Internet usage to ensure compliance with policies and standards and to identify and prevent inappropriate or malicious content. Internet usage and the content of files and emails are not private. Although limited personal use of the Internet is allowed, not all Internet sites will be accessible (i.e., sites that conflict with our security policy) and exceptions are not granted for personal use.

Further, delivery of email is not guaranteed; monitoring may result in the deletion or quarantining of any email content. All usage may be logged and retained and may be monitored at any time. As a result, you should use discretion and good judgment before using company property for personal use and should assume that any “personal” content will not be confidential.

Here are some basics to remember:

- All laws, regulations and company policies apply to your conduct when using information technology resources, including the Internet, the company Wi-Fi network, when using email and when posting content on social media. This includes those dealing with intellectual property protection, privacy, misuse of company resources, standards of conduct, sexual harassment, information security and confidentiality.

Remember, you are responsible for activity performed under your login credentials and when using the company Wi-Fi network. Never share your RACF and password with anyone.
Check with your management if you are not sure about your department’s policy. Information technology resources, including Internet and email capabilities, are provided to you at the sole discretion of management.

Exercise sound judgment when using information technology resources, including email and the Internet. This also includes publishing or posting content on social media websites (e.g., Facebook, LinkedIn, Twitter, YouTube, Pinterest). Employees should refer to our Social Media and Email, Internet, and Intranet policies for additional guidance.

Posting personal comments and/or opinions to the Internet, including social media websites, must not in any way imply that the opinions represent the opinions of the company.

Transmit confidential and proprietary information securely using approved encryption capabilities, such as secure email or secure file transfer.

Use approved mechanisms when sending protected health information (PHI) and other restricted confidential and proprietary data to outside entities.

Q: May I access Facebook from work?

A: Yes, Facebook and some other social media websites are accessible from your company’s desktop. However, use is at your management’s discretion and may involve occasional, brief activities and must not interfere with your job responsibilities. Remember, you must comply with all applicable company policies. Internet, Wi-Fi, and email usage is monitored and posting a file, comment or viewing content containing objectionable language (e.g., sexual, profane, racial, hatred) is not allowed. Employees are encouraged to use a personal device connected to the BlueWifi network to access Facebook and other non-business web services. Be advised that the BlueWifi network is subject to the same policies and content controls as the corporate network.
PROCUREMENT OF GOODS AND SERVICES

Part of protecting our assets includes making sure that our purchases of goods and services are done thoughtfully and make best use of our limited resources.

You are required to use company approved methods of procurement and contracting when purchasing business related goods, services and software. The goals of the company's Corporate Procurement policy and associated procedures are to ensure that best value purchases are made based on quality, price, service, reliability, compliance and risk, and other reasonable criteria. Additionally, there are special requirements of government contracts (e.g., Federal Employee Program) and programs that require the company to follow certain procurement practices when subcontracting for goods and services.

Here are some basics to remember:

• All purchases of goods and services must follow the company's Corporate Procurement policy and associated procedures.

• Agreements/contracts may only be signed by an employee at or above the level of vice president of the company/subsidiary that is named in the contract. Verify there is a valid agreement before providing any data or service.

• A business associate (BA) agreement or BA language must be included in the base agreement if PHI is being exchanged.

• Any documents provided to an external party promising anything on behalf of the company that require a signature/approval require review by Legal Affairs prior to signature/approval, except for agreements/contracts utilizing our standard terms.
and conditions (with no changes) that have been previously reviewed and expressly approved by Legal Affairs.

- Verify when the due diligence process is required and complete all aspects of the due diligence process.
- Avoid preferential treatment to vendors, suppliers and subcontractors for any reason (e.g., customer status, personal relationships). Doing so compromises the integrity of the procurement process and is illegal in some cases. It also creates a conflict of interest that may result in an arrangement that is ultimately not in the best financial interests of the company and may appear prejudicial to other customers and potential customers.
- Be aware of special circumstances or special requirements (e.g., Federal Employee Program, BlueCard, State Group) and their applicability prior to initiating the procurement process because additional due diligence and/or contract language may be required. Review the Corporate Procurement policy for these special circumstances.
- It is the responsibility of the signing officer to understand the provisions and obligations of the agreement/contract. Only an officer can legally bind the company to an agreement or contract.

Q: Our project team has been tasked with identifying potential cost savings through automation of work. I have found a perfect vendor that can help us with this. Corporate Procurement is evaluating several vendors, but I know my choice is the right one. The vendor representative has told me she needs to hear soon because other work is coming their way. I do not want her to lose interest, so I sent her a friendly email stating, ‘your company is still my top choice, and hopefully we will have you onsite in a matter of months.’ Is this OK?

A: No. This creates a situation in which the vendor representative knows she can get what she asks for, it also taints the bidding process, which can cause issues with state and federal regulatory agencies, and it limits Corporate Procurement’s ability to negotiate a fair arrangement for the company.
Here are some situations to always avoid:

- Engaging in discussions that could be construed as an agreement or creating an obligation on behalf of the company, or causing a potential vendor, supplier or subcontractor to think the employee, rather than Corporate Procurement or Legal Affairs, has authority to negotiate the arrangement.

- Suggesting that a vendor begin work or come onsite prior to finalization of the contract, or signing a contract, letter of intent or proposal without proper signature authority.

- Contracting with suppliers who are suspended, debarred or excluded from participation in any government procurement contract, grant program or health benefit program; procurement procedures also address suppliers that are excluded subsequent to entering into contracts with us.

- Sharing confidential purchasing or procurement information with a potential vendor, supplier or subcontractor, including source selection, scoring specifics, or internal documents evaluating them or their competitors.

- Accepting gifts, meals or entertainment from any persons or companies seeking to do business with our company.

**Q:** A potential vendor has offered to take our team out for lunch. We are currently involved in procurement activities with this vendor. Is this OK?

**A:** No. You must avoid even the appearance that procurement decisions are improperly influenced. Meals, gifts, or entertainment should not be accepted from persons or companies seeking to do business with our company.
CONFLICTS OF INTEREST

☐ Conflicts of Interest
CONFLICTS OF INTEREST

A conflict of interest (COI) may arise when personal interest or personal gain potentially influences or interferes with a business decision or other employment or professional responsibility.

A COI may arise as a result of your own outside activities or financial interests, or as a result of the activities or financial interests of family members or close personal or business associates. It is our goal to have our business conducted in such a manner so as to avoid even the appearance of a COI in our business dealings and relationships. You must avoid activities and situations that create a COI between personal or outside interests, including monetary interests, and the business interests of our company. The very appearance of a COI can create problems regardless of the intentions of the employee.

Here are some basics to remember:

- Disclose conflicts by completing a COI disclosure form when hired, annually and when your situation changes.
- Keep your COI disclosure form updated at all times with new disclosures as changes occur.
- As an employee or officer-level employee, owning individual shares of stock in a competitor company must be disclosed on your COI disclosure form.
- Disclose any situation where you have been convicted of a crime of dishonesty or a breach of trust.
- Contact your management, Legal Affairs, or Compass if you are not sure whether a situation is a COI.

To access the COI disclosure form start at the intranet home page and click:
- Quick Links
- Compass Program
- Conflict of Interest
- Complete My COI Disclosure Form

Compass Helpline 1-800-477-3736 X56300
• Employment or consulting opportunities for current or former government officials or employees are subject to conflict of interest laws and regulations. Consult with Compass or Legal Affairs before holding employment or consulting discussions with any current or former government official or employee.

• Be aware of, and comply with, the laws and regulations governing organizational conflicts of interest that may arise when dealing with government agencies and programs. For more information, refer to the Fair Competition and Business Ventures and Dealings with Government Programs and Interactions with the Public sections in this booklet.

Here are some situations to always avoid:

• Taking a leadership position or having a financial interest in an organization that competes with us or is a potential competitor.

• Entering into a business relationship with another person or business providing services to us.

• Becoming involved in another business relationship that requires such time or commitment that your duties here suffer.

• As an officer–level employee, owning individual shares of stock in a competitor (depending on an employee’s role, ownership of individual shares of stock in a competitor by a non-officer could also be considered a COI that you must disclose).
Q: I am a customer service representative and have an opportunity to take a second job in the admissions department of a hospital. Can I take the job?

A: In this situation, you will need to check with your manager and Compass or Legal Affairs before you take any outside position. There are certain guidelines that should be followed, and you will need to disclose this on your COI disclosure form.

Q: My sister is an employee here at our company. Should I report this?

A: Yes. You should disclose this on your COI disclosure form. Also, when completing the form, please provide as much detail as possible regarding your sister’s job.
7 GIFTS AND ENTERTAINMENT

- Gifts and Entertainment
- Charitable Giving and Community Investment
GIFTS AND ENTERTAINMENT

Offering or accepting business gifts or entertainment is generally discouraged because it creates a perception of an inappropriate relationship or conflict of interest even if the intent is innocent and there is no influence on your business judgment.

In addition to perception, there are various circumstances where the offer or acceptance of a gift, including anything of value, cash, entertainment, gift cards, tickets to events, travel, or other favorable treatment, is illegal or, at a minimum, creates a conflict of interest. When applying Compass Code of Conduct guidance as it relates to offering or accepting gifts, a good rule of thumb is to avoid offering or accepting any gift or business courtesy under any circumstance from or to firms or individuals conducting business with us. This includes competitors and those who would like to conduct business with us. In addition, you may not accept gifts that could suggest a conflict of interest, improper attempt to influence business decisions, or impair your judgment.

You may not offer any bribe, kickback, or other valuable consideration to anyone, including customers or members of their families, in connection with the sale of any of our products or services, or to obtain preferential treatment, secure or retain business or solicit an improper benefit personally or for the company.
Q: I received a gift card from a member as a thank you for recently helping her with an issue. I did not solicit the gift. Can I keep it?
A: No. Let your management know that you received the gift. Return the gift card to the member and inform her that our company policy does not allow us to accept gifts.

Here are some basics to remember:

- You may accept gifts of minimal value (such as occasional pens or paper pads) or perishable items that have already been received. (Perishable items should be made available to the entire department or returned. Tell the sender that it is against company policy to accept these gifts, and ask them to refrain from sending these items in the future.)

- You may accept reimbursement for, waiver of, or a discount on seminar fees and/or reasonable related travel and hotel when the waiver, reimbursement or discount is given in exchange for presenting or speaking at a conference or seminar or participating on a panel or focus group and, provided that, other similarly situated presenters are also provided with the waiver, reimbursement or discount.

- You may accept or provide modest meals and entertainment where the primary purpose of the meal or entertainment is business-related or related to your duties with the company, and the expense is reasonable and customary. It should also not suggest a conflict of interest or improper attempt to influence business decisions, including procurement activities. The employee as well as the external business representative or vendor must be present; otherwise, the meal or entertainment must be treated as a gift. Refer to the Offering and Accepting Gifts, Entertainment and Honorariums policy for guidance and certain restrictions.
• Dealing with government officials requires special attention. Under no circumstances may you offer gifts, meals or entertainment to any government official.

• Contact your management, Legal Affairs, or Compass if you have any doubts about a particular situation.

**Here are some situations to always avoid:**

• Accepting gifts or cash or cash equivalents from a member, customer, vendor, provider, physician or group administrator. If you are offered or receive a gift, either at home or at the office, tell your supervisor immediately. Return the item and inform the sender that our policy does not allow us to accept gifts. This includes gift cards, event tickets, trips, etc.

• Offering gifts or entertainment to influence any potential customers or any group administrator or person who has authority over an ERISA (Employee Retirement Income Security Act of 1974) health plan choice.

• Accepting gifts from or offering gifts to a government agency or public entity. This includes employees of the state, local government or a public entity, including a school board or a public hospital.

For more information on general guidelines to follow when dealing with government employees or officials, please refer to the Working with Government Customers section in this booklet.
Q: A vendor has invited me to a conference to learn more about its services and to hear testimonials from other clients. The conference is in another city, but the vendor will pay for my airfare, hotel, car and food expenses. Taking our budget into consideration, this will help in minimizing our travel expenses. Is this OK?

A: No. You must avoid even the appearance that your decision to procure the vendor’s services is improperly influenced. If there is a business need, our company can pay for the expenses.

CHARITABLE GIVING AND COMMUNITY INVESTMENT

Our corporate contributions program is based on the belief that, as a corporate citizen, we have an obligation to respond to community, economic and social needs.

We support qualified charitable organizations with financial and non-financial assistance (e.g., employee volunteers). To maximize the impact of our resources, Corporate Social Responsibility coordinates our company’s charitable efforts and concentrates on influencing a select number of community concerns. A streamlined, strategic approach to
distributing our charitable resources allows us to help those we serve in a meaningful way. For guidance on community service activities and organizations that may be supported by the company, please refer to the Corporate Community Investments and Employee Charitable Giving policy.

**Here are some basics to remember:**

- Make sure to forward all inquiries about community investments to Corporate Social Responsibility.

- Do not make any commitments for community investments without consulting with Corporate Social Responsibility.

- Follow all relevant company policies and procedures when using Volunteer Time Off (VTO) or volunteering as a representative of the company.

- When budgeting, do not include charitable donations and community investments in non-Corporate Social Responsibility cost center budgets including expenses such as travel, entertainment or other business-related expenses.
8 ACCURATE COMPANY RECORDS AND FINANCIAL INTEGRITY

- Accurate Record Keeping
- Travel
ACCURATE RECORD KEEPING
Federal and state laws and regulations require our contracts with government and non-government customers and our financial reporting and records to accurately reflect our business transactions.

We have a system of internal controls, which includes policies, procedures and internal and external audits to help ensure that business transactions have appropriate approvals and are properly recorded. However, it is your responsibility to ensure the accuracy of data, records and reports, whether for internal or external purposes. You must promptly report any inaccuracies or discrepancies to your management or to Compass.

We are required to retain records for a variety of our regulated activities and contracts, but it is also a good business practice to retain records in a consistent, systematic and reliable manner.

All company payments and other transactions must be properly authorized by management in accordance with company policies and procedures, and accurately and completely recorded in our company’s books and records in accordance with generally accepted accounting principles.

Under no circumstance may you create a false or misleading record or entry in any company record or report, or submit any false record, data, report or claim to anyone. Such activities can have serious criminal and/or civil legal consequences and would be considered employee misconduct, as would creating a record that was false or misleading by the omission of a material fact or data element. Permanent entries in company records should not be altered in any way and any corrections to any record must be made in good faith, with supporting justification, and approved, in advance, by your manager.

Accurate record keeping also includes ensuring that all contract and consulting expenses,
travel, timesheets and any other business related expenses and supporting data are accurate and complete, including ensuring the proper allocation of costs. Failure to make an accurate record and submission could result in a violation of our agreement with business partners and customers, including government agencies, or violate certain laws and regulations.

**Q:** I suspect that the financial report my coworker is accountable for contains discrepancies and may not be an accurate reflection of our financial records. I have questioned the inaccuracies before but nothing seemed to change. What should I do?

**A:** The company must have a financial accounting framework that can generate reports that are readily verifiable with traceable data. The accuracy of our company's financial records and the proper functioning of our internal accounting controls are vital to the company. Discrepancies or issues must be reported. If you are comfortable doing so, talk to your management about it to make sure you understand the situation. You can also contact Compass.

**Here are some basics to remember:**

- Disclose and record all corporate transactions. "Off-the-book" transactions are not allowed.
- Protect and regularly compare all company assets to ensure they are the same as what is actually on hand. Any variances should be reconciled.
- Monitor fraud, waste and abuse by using the controls in place to aid in the detection, investigation, and prevention of such activities.
- Cooperate fully and honestly with internal and external auditors.
- Report immediately any suspected fraud, waste or abuse involving our employees to Compass, Legal Affairs or an Employee Relations consultant.
• Report immediately any suspected fraud, waste or abuse involving providers, subscribers, agents or other persons, who are not our employees. You should notify the Special Investigation Unit (SIU) by calling 1-800-678-8355 or emailing specinvestunit@floridablue.com.

• Cooperate fully with any SIU investigation. The SIU is authorized to investigate allegations of fraud, waste and abuse. The SIU is also authorized to investigate business dealings that our company may have with outside contractors, consultants or vendors.

Here are some situations to always avoid:

• Placing company funds in a personal or non-corporate account.

• Intentionally causing any record to be inaccurate. Examples of prohibited acts include:
  - Making records appear as though payments were made to one person when they were made to another.
  - Submitting expenses for reimbursement which do not accurately reflect the true nature of the expense.
  - Falsifying time in the timekeeping system by recording time as worked when you are not working, or by working “off the clock.”
  - Changing the recipient on a claim to channel payments to an improper recipient.
  - Deleting claims from the computer system without rerouting for reprocessing and properly documenting the action.
  - Creating any other record which does not accurately reflect the true nature of the transaction.
Fraudulently influencing, coercing, manipulating or misleading any auditor engaged in auditing our company. These audits include, but are not limited to, audits of our company’s financial statements, audits of government programs and SOC-1 and SOC-2 audits of the company’s operations.

Q: I suspect my co-worker is falsifying his timesheets. What should I do?
A: Falsification of any company records, financial or otherwise, is not acceptable. The company has programs in place to help employees when times are difficult. Talk to your management about this and contact Compass.

TRAVEL
All business expenses must be documented promptly with accuracy and completeness on expense reports.

Here are some basics to remember:

- Report expenses within 60 days after returning from business travel.
- Get approval from your management for reimbursements.
- Employees are required to use the Company’s travel management company to book through the designated and supported online travel system.
• All supporting receipts must be attached to expense reports.
• Employees are not authorized to approve expenditures that they have initiated or incurred.
• Misuse of the Corporate Card will be subject to privileges being suspended or revoked as outlined in the Corporate Credit Card Policy 2.40.
• Personal charges on the Corporate Card are not allowed as outlined in the Corporate Travel and Business Related Expense Reimbursements Standard Operating Procedure 3.10.1
• Ensure expenses have a business purpose and are reasonable and necessary.
• Review all meals and other expenses charged to lines of business that allocate to any government contract or program to ensure that the expenses are allowable under the applicable rules.

Q: My co-worker recently traveled for business purposes, and I suspect she is falsifying her expense reports by claiming personal expenses that should not be reimbursed by the company. She feels the company owes her money, and this was her way of balancing things out. Should I report this?

A: Yes. Expenses must have a business purpose and falsification of any company record is not allowed. Talk to your manager about this and contact Compass.
PROTECTING INFORMATION AND PROPERTY

- Privacy
- Confidential, Proprietary and Other Non-public Information
- Employee Data and Verification of Employment
- Retention of Records
- Copyrights
- International Travel Restrictions
- Protecting Our Brands
We must safeguard and protect our company's confidential and proprietary information. Additionally, we have a legal and ethical obligation to safeguard and protect the confidential information of our customers and business partners. We must respect the intellectual property rights of others.

Q: I know that safeguarding PHI is important, but don't we go overboard with our controls?

A: No. Improper uses and disclosures of PHI can invade someone's privacy, damage reputations, cause embarrassment, violate federal and state privacy laws, invite lawsuits and violate corporate policies and procedures. Improper uses and disclosures of PHI may also be violations of our company’s agreement or contract with a government agency and/or another customer. Federal and state privacy laws carry significant penalties for violations. These penalties may apply both on a corporate and individual basis.

PRIVACY
We comply with all applicable federal and state privacy laws.

Here are some basics to remember:

- Learn and comply with our Corporate Customer and Consumer Information Privacy policy and related standard operating procedures and any contractual obligations that may apply.
• Protect all health, financial and/or employment information. This includes information such as names, addresses, telephone numbers or any other data that can be used to identify an individual. Such information may only be accessed, used and/or disclosed as permitted by state and federal privacy laws and/or policies and procedures.

• Limit access, use and disclosure of information to the minimum amount of information necessary to achieve the intended purpose of the access, use or disclosure.

• Use de-identified data whenever possible.

• Use of Social Security numbers internally or externally is prohibited unless there is an approved compelling business need.

• Retaliation against an employee for reporting privacy-related or other concerns is a violation of our Compass Code of Conduct.

• Report any known or potential breach of privacy or non-permitted use or disclosure of information to Business Ethics, Integrity & Compliance immediately. This includes any loss or theft of information.

• Ensure disclosure of information is only to an authorized individual or entity.

• Get permission to use employee information or member information.

• Check for accuracy of information.

• Send all PHI securely via secure file transfer or by typing the word "secure" on the subject line in emails.
Q: A vendor of the company has requested a list of our members who are diabetic. This information is necessary for the vendor to fulfill its contractual obligations. Is it OK for me to provide the vendor with the requested member information?

A: It depends. PHI should always be protected and not disclosed or shared without ensuring proper approvals are in place. Contractual agreements such as a business associate agreement and/or other agreements are required. In addition, approval through the formal governance process may be required. If you are unsure about the approval process, contact Business Ethics, Integrity & Compliance (BEIC) for guidance.

Here are some situations to always avoid:

- Sharing information with someone who is not authorized to receive it, both internally and externally.
- Accessing information that is not needed for your job function.
- Not using caution when sharing information via email, fax, mail or other distribution means.
- Not protecting information that could result in a non-permitted disclosure, including inadvertent ones that could arise in social conversations or in business relations with individuals outside the company.
- Not protecting information that could aid others in the commission of fraud, waste, abuse or misuse of company products or services, or invasion of privacy.
Q: I need to update and save a spreadsheet that contains PHI. Can I save this to an unrestricted team site?

A: No. PHI or other sensitive information should never be stored on an unrestricted team site. These documents should only be stored on a restricted team site, or your H, I or J drives, as appropriate.

CONFIDENTIAL, PROPRIETARY AND OTHER NON-PUBLIC INFORMATION

It is our policy to require all employees to respect the sensitive nature of company confidential and proprietary information.

Confidential, proprietary and other non-public information that you obtain about our company, customers and vendors is often subject to non-disclosure agreements or policies and specific privacy laws and regulations. The disclosure or personal use of such information may also violate trade secrets, securities and procurement laws and regulations. You are prohibited from using any unlawful or deceptive means to seek or obtain confidential, trade secret or other non-public information of competitors or regarding competing products and services.

Here are some basics to remember:

• When joining the company, you are required to sign a statement that assigns the
company all rights, if any, in intellectual property that you may develop or create in the discharge of your duties.

- You are required to acknowledge that you understand and will follow the company’s Classification of Information policy, even after your employment with the company has ended.

- You may not disclose or use at any time, either during or subsequent to your employment, any confidential and proprietary information gained during your employment, whether or not developed by you, except as required to perform your duties as an employee of the company.

- You must promptly return all company property upon termination, including all manuals, letters, notes, notebooks, reports and all other confidential and proprietary materials.

- Violations by an employee or former employee may result in disciplinary and legal action. If you have questions about whether a particular matter is restricted, contact Compass or Legal Affairs.

Q: I saw an article on the GuideWell intranet that I would like to share with a family member. Is it OK to give it to them?

A: No. Although unrestricted confidential and proprietary information can be shared with company employees, approval is required to share or disclose this information with individuals or organizations outside of the company.
EMPLOYEE DATA AND VERIFICATION OF EMPLOYMENT

The company recognizes the importance of privacy and confidentiality with regard to employee information.

We generally do not allow disclosure of employee information to third parties outside the company unless:

- The employee authorizes the disclosure;
- A court orders such disclosure; or
- The company is under some other obligation to make the disclosure.

Here are some basics to remember:

- Protect employee information from unwarranted exposure by providing only the minimum amount of information necessary to accomplish the intended task.
- Access to or use of any employee information is allowed only on a documented, need-to-know basis and must only be used to support the specific business function for which access was granted.
- Follow normal business processes when dealing with your personal insurance-related business and do not request that others in the business intervene to assist you.
- When asked to provide employment references, refer the individual to the Automated Employment Verification Information Line which is available 24 hours a day, seven days a week, by telephone or Internet. Our company will confirm an individual’s dates of employment, job title and salary.

Never share employee information with other employees unless there is a business reason and it is within their designated scope of duties.
Here are some situations to always avoid:

- Using employee information as test data, for training purposes or to provide examples or testimonials, unless the employee completes the appropriate authorization form.

- Bypassing normal operating procedures. Any requests to do so should be reported to Business Ethics, Integrity & Compliance.

RETENTION OF RECORDS

It is good business practice to retain information assets (i.e., data, information, documents and records) in a consistent, systematic and reliable manner so that they can be retrieved promptly when required.

Failure to keep records in good order can result in adverse consequences for the company. All employees who create, receive, use or manage the company’s information assets must comply with the Records Management and Retention policy.

Q: Our department is moving to an office space within our company, and I no longer have use for the documents from previous years. Can I just dump them in a blue bin?

A: No. You need to review the documents to determine if they are records and if they are subject to a retention period or a legal hold. If unsure, talk to your management or contact the Enterprise Records Manager in Legal Affairs.
Here are some basics to remember:

- All information assets regardless of storage medium or storage location, are subject to a retention period.

- Records may be: (a) paper documents, forms, reports, manuals, correspondence, and files; (b) computer files, such as spreadsheets, word-processed documents and email messages; or (c) information in other formats, such as video streams, audiotape, microfilm and photographs.

- Make sure you manage, retain and destroy all company-owned information assets business records in a manner that supports both ongoing business operations and compliance with various accounting, audit, customer, legal, regulatory and tax requirements. See the Records Management and Retention policy and the Records Retention Schedule for guidance.

- Follow legal hold notices issued by Legal Affairs. In certain cases, a legal hold notice is sent out by Legal Affairs suspending retention requirements for certain documents and records. A legal hold notice requires preservation of certain documents and records under special circumstances, such as pending or actual litigation, government investigation, audits or consent decrees and supersedes the requirements of the Records Management and Retention policy for the duration of the legal hold.

- Do not destroy, discard, withhold or alter documents and records pertinent to a legal matter, governmental audit or investigation. Criminal penalties can result from these actions.
Q: To be on the safe side, whenever I create an important document, I mark it “permanent” for retention. Is this OK?

A: No. Few documents actually require permanent retention and retaining a document longer than necessary is not compliant with the Records Management and Retention policy. To ensure you are applying the correct retention period, please familiarize yourself with the Records Retention Schedule on the Records Management intranet site, which you can access from the intranet home page under Employees.

COPYRIGHTS

The computer software that we develop and license is protected by copyright, as are the written and audio-visual materials we develop, purchase, lease or license.

Copyright holders have certain rights, protected by law, that prohibit the unauthorized duplication, distribution, performance and other uses of copyrighted works. In the digital age, it is much easier to create, use, copy and distribute information than in the past, but many people are unaware of the copyright restrictions and responsibilities that arise when using the media materials that seem almost universally available. As an employee, you must respect computer software copyrights and adhere to the terms and conditions of all software licenses to which our company is a party.

Here are some things to remember:

- Violating the rights of copyright holders is a breach of ethical conduct and could expose you and the company to significant legal penalties.

**Compass Helpline** 1-800-477-3736 X56300
• Only licensed software acquired through the appropriate procedures may be used on our computers.

• Corporate-owned software must not be installed on your home or personal computer unless specifically approved for use, such as corporately approved virus protection software.

• Ensure that you have permission before you use or copy any media, including computer programs, music, photos, drawings, articles, movies, etc.

• Media and materials on the Internet are not in the “public domain” and are not exempt from copyright protections merely because they are publicly available.

Q: I found some photos and music on the Internet that I would like to use in my presentation. Can I use these materials?

A: No—at least not without permission. This type of intellectual property is generally protected by copyright law as are books, articles, magazines and music. Permission must be granted from the copyright holder for most uses and that permission sometimes requires a fee or some other royalty payment arrangement with the copyright holder or someone acting on their behalf.
INTERNATIONAL TRAVEL RESTRICTIONS
If you support our company in activities that require international travel or transactions with international business partners, you must ensure that you understand the export restrictions and requirements related to your activities.

Taking or sending company equipment, including laptop computers, and the transfer of technical data overseas may require license approval from the federal government. The deemed export control laws may also apply, depending on the type of technology or software, if used by foreign national employees or contingent workers. At a minimum, you should know the export category and any applicable exemption for your technology or software if you travel for work or if you are a foreign national.

If you have questions about matters related to international travel restrictions, contact Business Ethics, Integrity and Compliance or Legal Affairs.

PROTECTING OUR BRANDS
We have an Enterprise Brand policy in place to ensure our company’s activities are in alignment with our enterprise brand strategy and in compliance with legal requirements.

It provides guidance for brand use in communications that contain any reference to our company or are seen as coming from the company or one of our subsidiaries and/or affiliates.
We have also developed brand guidelines that describe the core elements of our corporate identity and provide examples of their application. They are intended for use by our company and its employees and by external designers, printers, advertising agencies and other consultants who design, create or produce communications or products bearing our brands. The correct application of our guidelines is essential to maintain the integrity of our brands, as any deviation will weaken the overall brand image. Brand guidelines and downloadable brand assets can be found on the GuideWell Brand Center at guidewellbrandcenter.com.

Here are some things to remember:

- The Enterprise Brand policy is designed to protect the brand value of the company’s symbols and the reputation of our name. It guides us in delivering on our mission and living up to the key attributes that define our company’s personality and purpose. Use it to communicate a consistent message in tone, look and feel across multiple media and to our diverse audiences.

- Advertising and promotion of our company, subsidiaries, products and services must be reviewed in advance by both Enterprise Brand and Legal Affairs.

If you need assistance or have a question regarding brand use, please contact Enterprise Brand at Brand-GuideWell@guidewell.com or brand@floridablue.com.

Q: One of our vendors would like to use our company logo in its promotional materials. Can I give the vendor a logo to use?

A: Maybe. It depends on the nature of the relationship with the vendor, the services it will perform and for which company it will be performing services. Our brands are vital to the company. There are strict guidelines to follow. Consult with Enterprise Brand or Legal Affairs for guidance.
INFORMATION SECURITY

- Information Security
INFORMATION SECURITY

We protect our technology and information through a combination of policies, standards, procedures and technology. Ongoing monitoring of information and system access and use is routinely performed for appropriateness, unauthorized activity, new threats and opportunities for improvement.

Information assets are secured according to classification level as defined in our policies. If you are uncertain about the classification level for any particular use of information, it is our policy to protect the information at the highest level of classification. Employee access to protected information is limited based upon the job function of the employee and the classification of the information requested. You will be required to provide access and authentication credentials prior to accessing protected resources.

Here are some basics to remember:

• Identify information as confidential restricted, confidential restricted proprietary, or confidential unrestricted depending on the legal requirements and business agreements needed to protect it.

• Limit sharing and use to those who need to know, and limit access based upon job role.

• Get appropriate approvals, authorization or contractual arrangements before sharing information with anyone outside of the company.

• Store information according to its classification.

• Never store confidential and proprietary information on a personal mobile computing device.
• Lock your workstation when away from your desk (CTRL+ALT+DEL) or Windows key + L.

• Physically secure your laptop or portable device(s). Use extra care to protect mobile devices when traveling. Never leave mobile items in an unlocked car.

• Report lost, stolen or damaged computing equipment, portable devices or media immediately to Safety and Security.

• Keep your login credentials secure and never share with others.

• Choose complex passwords that are not easily guessed.

• Email and Internet use is monitored.

• Be alert to cybersecurity defenses and do not fall victim to phishing emails.

• Be skeptical of unfamiliar emails or requests for your login credentials.

---

**Q:** I received an email that appears to be from our company. It is asking me to click a link and provide my password. Is it OK for me to provide this information when asked to do so?

**A:** No. If you receive an email that appears to be from our company and asks for your corporate user ID and password, this is a phishing email and should be reported immediately to the IT Service Desk. However, there are occasions when you may receive an email from one of our company’s vendors asking for a user ID and/or password. In this case, you will use a user ID and/or password that you have created with the vendor to register for a specific purpose such as a corporate meeting request.
Dealings with Government Programs and Interactions with the Public

- Working with Government Customers
- Political Contributions and Lobbying Activities
- Activities Abroad
WORKING WITH GOVERNMENT CUSTOMERS

We conduct business with the U.S. government and various state and local government entities and agencies. The laws and regulations that govern those activities are strict and often complex. Therefore, all employees must be aware of and abide by all laws, regulations, rules and other requirements that govern the conduct of government programs, contracts and associated transactions.

If you are unsure about the applicable legal, regulatory or contract requirements in a particular situation, contact Business Ethics, Integrity & Compliance or Legal Affairs for guidance. Interacting with government agencies and officials also requires a continuing commitment to the highest ethical standards, attention to detail and significant due diligence in order to protect the company’s reputation and on-going participation in government markets.

Here are some basics to remember:

- Always be accurate and truthful when interacting with government agencies and officials. Documents and other records provided as well as oral or written representations made to the government must always be clear, complete and not misleading.
- Cooperate fully and honestly with government audits and inquiries.
- Never give/receive payments, or anything of value, to or from anyone in exchange for referrals for services paid under a federal health care program.
- Adopt and follow controls and processes that ensure the accuracy of data and
representations communicated to the government and/or used in connection with government contracts and/or government programs.

- Ensure consultant, vendor and supplier adherence to government requirements and company policies and contract terms.

- Ensure that charges to government contracts and the use of appropriated funds are accurate and authorized, including ensuring that work time is accurately recorded and unallowable expenses are excluded.

- Promptly report to Business Ethics, Integrity & Compliance or Legal Affairs activity that you believe is unlawful, would result in a false claim, or would result in an overpayment by the government to us or in the retention of funds that are owed to the government.

- Conduct appropriate due diligence on prospective suppliers and vendors.

- Never accept gifts from or offer gifts to a government agency or public entity. This includes employees of the state, local government or a public entity, including a school board or a public hospital.

- Violation of the laws and regulations regarding gifts to government employees can result in serious criminal and/or civil legal consequences. You should also remember that a violation of any law or regulation can result in disciplinary action up to and including termination of your employment.

**Here are situations to always avoid:**

- Deviating from contract requirements without proper written approval from an authorized government official.

- Offering, promising, or giving a gift, cash, or anything of value to a government employee or official.
Q: The company is thinking about how to create new provider arrangements that give incentives to providers for better managing the outcomes of our members and increasing their patient base. Is it OK for me to negotiate as part of the arrangement that our company compensates the provider group for an increase in our company’s membership?

A: No. An arrangement that offers payment in return for referrals of patients may be prohibited. Check with Legal Affairs for guidance on how to proceed with this proposed arrangement. You can also contact Compass.

- Requesting or accepting gifts, cash, or anything of value from a government employee or official.
- Engaging in employment discussions with a government official who has decision-making or procurement responsibility for contracts with the government. Because there are significant restrictions regarding employment discussions with current and former government employees and officials, consult with Business Ethics, Integrity & Compliance or Legal Affairs prior to engaging in any such discussions.
- Accepting or seeking to obtain non-public source selection or competitive information about government procurement or a competitor’s bid or proposal.
- Hiring or contracting with individuals or entities that are excluded from federal procurement and non-procurement programs for performance under any government contract or program, including the Federal Employees Health Benefits Program (FEHBP) and Medicare.
Q: We are seeking to expand our government business segment. Several government officials will be in town and have offered to meet with us for dinner. To thank them for their time, we think it would be a nice gesture to pay for their dinner. Is this OK?

A: No. Offering anything of value, including meals, to a government employee or official is not allowed.

POLITICAL CONTRIBUTIONS AND LOBBYING ACTIVITIES

We encourage all employees to vote and be active in the political process.

Federal and state laws, however, limit the nature and extent of individual and corporate political participation. For example, federal law prohibits corporate contributions to federal political candidates or office holders. State law limits corporate contributions to candidates for state or local office to $500 per candidate per election.

We maintain our non-partisan political action committee, the Florida Health Political Action Committee (FHPAC), as one way that eligible employees may voluntarily participate in the political process. Political contributions made by FHPAC are funded entirely by voluntary contributions from eligible employees. FHPAC’s activities are regulated by the federal government, including detailed disclosure requirements with the Federal Election Commission. These reports are publicly available and include an itemization of all
receipts and disbursements, including any political contributions, over a certain amount. Participation is completely voluntary at the discretion of eligible employees.

Lobbying is broadly defined to include making contact with government officials and officers regarding legislation, rules, regulations, programs and the award of contracts. It does not include routine contacts made in the course of normal government business like the administration of a government contract (including submission of a proposal), responding to a government request (including requests for comments on rulemaking), responding to legal process, or filing required reports.

It is not only important to comply with existing laws and to be aware of restrictions and requirements regarding political activities and contributions, but due diligence in keeping track of lobbying activities and contributions is required in order for the company to accurately certify to cost submissions and file lobbying disclosure reports related to government contract awards and participation in government programs.

**Here are some basics to remember:**

- The political process is highly regulated.
- No reimbursements are allowed for personal political contributions, including contributions to political action committees.
- Do not work on political campaigns during work hours.
- Do not use company resources, such as telephones, copy machines, email, and fax machines, as part of a campaign effort, including fundraising.
- Make sure you direct questions to Public Affairs and Community Engagement’s Government Relations area before agreeing to do anything that could be construed as involving the company in any political activity at the federal, state or local level.
Here are some situations to always avoid:

- Soliciting political contributions on company property is not allowed. (Our FHPAC may solicit eligible employees on company property during work time.)
- Distribution of literature on company property or use of company assets for political purposes is not permitted.

Q: I am a volunteer for a political candidate. Is this OK?
A: Yes, as long as your activities are done on your own time, at your own expense, and without the use of company assets.

ACTIVITIES ABROAD
For those employees involved in international activities and transactions, there are additional rules to follow. It is of critical importance that employees understand it is a criminal violation of U.S. law to pay or promise to pay or give cash or anything of value to a foreign official in order to obtain or retain business or receive favorable treatment. This applies to our employees and our business partners working overseas on our behalf.
Certain programs, products and accounts do not permit the offshoring of services to be performed or may require prior approval for it to occur. Offshoring refers to our company’s use of a vendor that provides all or some of the services for us outside the borders of the United States. Know the requirements of the programs, products and accounts you are working on. Check with Legal Affairs or Business Ethics, Integrity & Compliance immediately if you become aware of offshore activities involving our State Group, Federal Employee Program or Medicare business.
LEGAL AND
REGULATORY
REQUIREMENTS

Legal and Regulatory Requirements
LEGAL AND REGULATORY REQUIREMENTS

We are subject to many state, federal and, in some cases, even local laws and regulations that apply to our business. Although not inclusive, the following are some of the laws with which you should become familiar. As with any law or regulation, if you question whether a particular law or regulation applies to our company or have concerns that we are not fully complying with a law or regulation, you should consult with Business Ethics, Integrity & Compliance or Legal Affairs.

Our Environment

Age Discrimination in Employment Act
The Age Discrimination in Employment Act prohibits discrimination on the basis of age in hiring, promotion, discharge or other privileges of employment by any applicant and employee 40 years of age or older.

Americans with Disabilities Act of 1990
The Americans with Disabilities Act prohibits discrimination on the basis of disability in employment, governmental activities, public accommodations, transportation and communications.

Civil Rights Act of 1964 (Title VII)
Title VII of the Civil Rights Act prohibits discrimination on the basis of race, color, religion, sex or national-origin. Title VII also prohibits discrimination against an individual because of his or her association with another individual of a particular race, color, religion, sex or national origin.
Fair Labor Standards Act of 1938
The Fair Labor Standards Act of 1938 mandates a basic minimum wage and overtime pay for most private and public employers. It also prohibits the use of workers under the age of 16 in most jobs and the use of workers under the age of 18 in those occupations deemed dangerous.

Executive Order 13627- Strengthening Protections Against Trafficking in Persons in Federal Contracts
The Executive Order requires federal contractors to adopt and enforce a zero tolerance policy regarding trafficking in persons, which includes prohibitions in engaging in severe forms of trafficking in persons, procuring commercial sex acts, or the use of forced labor in the performance of the contract.

Florida Whistleblower Act
This Florida Whistleblower Act protects employees from any form of retaliation when they disclose information about actual or suspected violations or misconduct.

Dealing with the Marketplace and Business Partners

Antitrust Laws
Federal and state antitrust laws prohibit business practices that unfairly deprive consumers of the benefits of competition. Without competition, consumers may pay higher prices for goods and services.

Protecting Information and Property

Copyright Laws
Copyright laws protect the original works of authors and artists and give exclusive rights
Health Insurance Portability and Accountability Act of 1996 (HIPAA)

HIPAA is a federal law that principally reformed the group health insurance market. HIPAA creates greater access to health care insurance, promotes standardization and efficiency in the health care industry, protects the privacy of health care information and sets standards for the security of electronic health care information.

Dealing with Government Programs and Interactions with the Public

Anti-Kickback Statute

The Anti-Kickback Act prohibits knowingly and willfully soliciting, receiving, offering or paying remuneration, including any kickback, bribe, rebate, or anything of value, for referrals for services that are paid, in whole or in part, under a federal health care program or is provided to any federal contractor or subcontractor for the purpose of improperly obtaining or rewarding favorable treatment in connection with a federal contract or subcontract.

Bribery and Gratuities

Federal law makes it illegal to directly or indirectly offer or promise anything of value to a public official with the intent to influence an official act (bribery) or to offer or promise anything of value to a public official “for or because of” an official act (illegal gratuity). No corrupt intent is required in order to be considered an illegal gratuity and the statute prohibits gratuities for past and future official acts.

Excluded Parties

As a general rule, federal contractors and federal health program participants are prohibited from entering into contracts with and making payments to parties suspended or debarred.
from procurement and non-procurement programs and parties excluded from participation in federal health care programs. This includes for items or services furnished, ordered or prescribed by an excluded individual or entity.

**Federal and State False Claims Acts**
Federal and state false claims acts prohibit the knowing submission of a false claim or causing another to submit a false claim payable under a federal or state program. This includes knowingly submitting inaccurate data under a federal program. In addition, the failure to return any overpayment of government funds may also be a false claim.

**Foreign Corrupt Practices Act**
The Foreign Corrupt Practices Act prohibits certain classes of persons and entities from, directly or indirectly, paying or offering, bribes, kickbacks, or other payments of money or anything of value to anyone, including officials, employees, or representatives of any government, company, or public or international organization, or to any other third party, for the purpose of wrongfully obtaining, retaining or directing business.

**The Stark Law (Physician Self-Referral Law)**
The Stark Statute, otherwise known as the Physician Self-Referral Law, prohibits a physician from making a referral for certain designated health services to an entity in which the physician (or a member of his or her family) has an ownership or investment interest or with which he or she has a compensation arrangement.

**Other**

**Affordable Care Act**
The Affordable Care Act includes many reforms that have overhauled the U.S. healthcare system, including the establishment of health insurance exchanges, the elimination of
pre-existing condition exclusions and lifetime maximums, the requirement that individuals who do not have insurance must buy insurance or pay a tax (individual mandate), and the availability of cost sharing subsidies and premium tax credits, among numerous other provisions.

**Section 1557 of the Affordable Care Act**
Section 1557 prohibits discrimination on the basis of race, color, national origin, sex, age, or disability in certain health programs and activities.

**Florida Insurance Code**
In conducting our health insurance and HMO businesses, we must comply with all applicable provisions of the Florida Insurance Code and regulations duly promulgated from time to time by the Florida Office of Insurance Regulation, the Florida Department of Financial Services, and the Agency for Health Care Administration.

**Telephone Consumer Protection Act**
The Telephone Consumer Protection Act (TCPA) is a federal law that restricts use of an automated telephone dialing system for certain types of telemarketing activities. TCPA implemented the national Do-Not-Call list in 2003.