

2026

COMPASS

Code of Ethical Business Conduct

Guiding Integrity and Ethics



UPDATED: FEB 2026

GUIDEWELL

GuideWell Mutual Holding Corporation

Leadership Messages



Health care is under real pressure, and the people and communities we serve feel it every day. When they choose GuideWell, they place their trust in us at some of the most vulnerable moments of their lives. Earning that trust is one of our most important responsibilities, and it's defined by the choices we make when the stakes are high.

Our Compass Code of Ethical Business Conduct (Code of Conduct) is how we show people who we are. It sets clear expectations for how we treat one another, how we use information, how we manage resources, and how we uphold the law. Compliance is how we protect the privacy, dignity, and financial security of the people who rely on us. It's how we operate with honesty, even when it's uncomfortable, and anchor our performance in compassion. As we move forward, we must always do so responsibly and with care. That is the culture we're intentionally building together.

Trust grows when our values show up in action: telling the truth, refusing shortcuts, speaking up when something does not align with those values, and seeking guidance before we act. Everything we do sends signals about who we are, and those signals must reflect our accountability and integrity. There is no trade off between doing what's right and delivering results. We are accountable for both.

Thank you for taking our responsibilities seriously and for doing the right thing, especially when it's hard. That's how we strengthen trust and remain a partner our communities can count on.

A handwritten signature in black ink, appearing to read 'Brian Pieninck', written in a cursive style.

Brian Pieninck
President and CEO



At GuideWell, integrity and compliance are shared responsibilities. Our Code of Conduct exists to protect our employees, customers, patients, and the mission we serve.

We must act ethically — not only because it's the right thing to do — but because the risks and consequences of failing to do so are far-reaching. Every decision matters, and each of us plays a role in safeguarding the trust placed in our organization.

The Code of Conduct is our promise — to act with transparency, accountability, and courage in every situation. When we uphold these standards, we reduce risk, protect our reputation, and strengthen GuideWell for the future.

A handwritten signature in black ink, appearing to read 'Colleen D. Brennan', written in a cursive style.

Colleen D. Brennan
Vice President, Chief Integrity, Compliance and Risk Officer

Our Values

The beliefs and priorities that drive our company's culture



LEAD

Listen deeply.
Act courageously.



SERVE

With hustle.
With heart.



IMAGINE

Go bold. With
discipline and data.



DELIVER

We say it.
We own it.
We do it.



UNITE

One team.
Shared purpose.



EVOLVE

Always striving.
Ever improving.

Table of Contents

Integrity and Ethics	6
Our Commitment	7
Why We Have a Code of Conduct	7
Individuals and Entities Subject to the Code of Conduct	7
Disciplinary Action	8
Why Ethics, Integrity and Compliance Matter	8
Our Ethical Decision-making Framework	9
Our Responsibility and Reporting Concerns	11
Our Shared Responsibility	12
Management Responsibility	12
Reporting Situations	13
We Will Not Tolerate Retaliation	14
Our Environment	15
Maintaining a Safe Work Environment	16
Human Rights	17
Inclusion	17
Discriminatory and Sexual Harassment	17
Equal Employment Opportunity	19
Soliciting and/or Distributing Literature	20
Environmental Standards	21
Dealing with the Marketplace and Business Partners	22
Fair Dealing and Competition and Business Ventures	23
Advertising and Marketing	25
Conflicts of Interest	26
Conflicts of Interest	27

Table of Contents

Gifts and Entertainment	28
Gifts and Entertainment	29
Charitable Giving and Community Investment	31
Accurate Company Records and Financial Integrity	32
Accurate Record Keeping	33
Retention of Records	36
Protecting Information and Property	37
Cybersecurity	38
Privacy	39
Confidential, Proprietary and Other Non-public Information	41
Employee Data	42
Use of Company Assets	43
Company Assets	44
Internet, Email and Social Media	45
Artificial Intelligence (AI)	46
Information Security	47
Information Security	48
Dealings with Government Programs and Interactions with the Public	49
Working with Government Customers	50
Political Contributions and Lobbying Activities	52
Activities Abroad	54
Legal and Regulatory Requirements	55
Legal and Regulatory Requirements	56
Resources	59



INTEGRITY AND ETHICS

- Our Commitment
- Why We Have a Code of Conduct
- Individuals and Entities Subject to the Code of Conduct
- Disciplinary Action
- Why Ethics, Integrity and Compliance Matter
- Our Ethical Decision-making Framework

OUR COMMITMENT

We are committed to conducting business ethically, with integrity and in compliance with laws and regulations.

Our goal is to advance our corporate culture of compliance, guided by the highest standards of integrity and ethical business conduct. Strengthening our commitment to compliance and ethics not only reinforces our values, but also distinguishes us as a company and provides us with a competitive advantage in the marketplace.

WHY WE HAVE A CODE OF CONDUCT

The Code of Conduct 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 supplements policies and procedures, which provide more detailed guidance on company expectations and requirements for behavior in the workplace and while conducting company business.

**All referred to as
“employees” in this
Code of Conduct*

INDIVIDUALS AND ENTITIES SUBJECT TO THE CODE OF CONDUCT

The Code of Conduct applies to GuideWell Mutual Holding Corporation (GMHC), certain wholly-owned subsidiaries, certain affiliates, and employees of the company. GMHC, certain wholly-owned subsidiaries and certain affiliates are collectively referred to as the “company.”

We are required to read, understand and comply with the Code of Conduct and all company policies and procedures. If your business area has policies or procedures that are more specific than the Code of Conduct, you should follow those policies or procedures. Likewise, in the event that the Code of Conduct conflicts with any law or regulation, you should follow the law or regulation.

DISCIPLINARY ACTION

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

Misconduct that is likely to result in disciplinary action includes, but is not limited to:

- Violating or directing others to violate the law, regulation, company policies or company procedures;
- Failing to promptly raise a concern regarding illegal, non-compliant or unethical activity;
- Failing to cooperate with investigations into allegations;
- Retaliating against an employee who has made a good faith report of potential misconduct or who has cooperated in an investigation; and/or
- Making an allegation in bad faith and/or other intentionally false allegation of misconduct.

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.

WHY ETHICS, INTEGRITY AND COMPLIANCE MATTER

Acting ethically with integrity and in compliance with laws and regulations is as important as any aspect of our business. It helps us uphold our commitment to our communities, our customers, and our patients. How we conduct ourselves reflects on us as individuals and the company.

We are expected to:

- Promote the safety and welfare of our fellow employees, our customers, and our patients;
- Encourage a cooperative and professional work environment;
- Protect personal rights and company property;
- Demonstrate the highest standard of integrity and ethical behavior; and
- Treat our fellow employees, our customers, and our patients with dignity and respect.

OUR ETHICAL DECISION-MAKING FRAMEWORK

When faced with an ethical dilemma, the best course of action may not always be clear. The Code of Conduct does not address every situation we could face, nor does it summarize all the laws, rules and regulations applicable to our company. Therefore, it is important to understand the principles behind the Code of Conduct and how to apply them.

The ethical decision-making framework is a series of questions to guide us when we are unsure about what to do in a situation. It is especially helpful when we are faced with a choice that does not feel right or when we are unsure if our actions align with what is right or wrong.

Consider the following questions when unsure whether an action or situation is appropriate:

Gain Clarity

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

Identify and clarify the ethics issue.

Consult Resources

- Does anything about this situation violate our Code of Conduct, company policies or procedures, laws or regulations?

Consult with your immediate manager or the human resources, compliance or legal department to determine whether a situation is inconsistent with our Code of Conduct, company policies or procedures, laws or regulations.

Consider the Consequences

- How will our employees, customers, patients or others be affected by this decision?
- What effect could this decision have on the company's reputation and on my own?

Focus on the impact decisions will have on others. Who has an interest at stake? Who will be helped or hurt by the decision? Would we want to read about this in the news?



RESPONSIBILITIES AND REPORTING CONCERNS

- Our Shared Responsibility
- Management Responsibility
- Reporting Situations
- We Will Not Tolerate Retaliation

OUR SHARED RESPONSIBILITY

We must question or challenge situations suspected of being unethical or in violation of company policies, company procedures, the Code of Conduct, laws or regulations. By doing so, we are protecting ourselves, our fellow employees, our company, our customers and our patients.

Here are some basics to remember:

- We should raise concerns or seek guidance if we are unsure or have an uneasy feeling about whether certain behaviors or activities are compliant or ethical.
- We must fully cooperate with any internal or external investigation.
- We are not expected to have the answer to every compliance or ethics question, but we are expected to know when to ask for help and where to go for help.

MANAGEMENT RESPONSIBILITY

All levels of management are expected to clearly articulate our commitment to compliance and ethics, lead by example, and not ignore non-compliant or unethical behavior.

Here are some basics to remember:

- All levels of management are responsible for:
 - o Understanding and enforcing the Code of Conduct;
 - o Maintaining an open-door environment where employees feel comfortable reporting unethical or non-compliant situations, regardless of what the outcome may be, without fear of retaliation; and
 - o Addressing compliance-related questions or concerns promptly and engaging the appropriate parties (e.g., human resources, compliance, legal) who can work toward a resolution, all while keeping confidentiality to the extent possible.

REPORTING SITUATIONS

Reporting activities that violate our Code of Conduct is the right thing to do. We should speak up, even if we do not have complete information about the situation.

First, discuss the situation with your immediate manager. If the matter is not handled to your satisfaction, or you are not comfortable talking to your immediate manager, there are additional ways to make an inquiry or report a situation without fear of retaliation. All reporting mechanisms are equal and, based on your preference or comfort level, you may use any one of them.

You may also ask a question or file a report confidentially or anonymously. If a report is made anonymously, be sure to provide enough information about the situation to allow for a thorough investigation. It is sometimes difficult to investigate situations without involving you, so you may be asked if you are willing to identify yourself. Our company has a non-retaliation policy to protect you.

Refer to the appendix for a list of available resources.

When making a report:

- Provide honest, verifiable facts and describe the situation in detail.
- Identify dates when the events occurred.
- Indicate if the activity was observed directly or found out through another source.
- Advise how the situation occurred (e.g., Was a policy not followed? Was someone told to do something inappropriate?).
- Provide relevant documents or supporting evidence that could help with the investigation.

Once you make a report, an inquiry/investigation will be initiated as quickly as possible.

WE WILL NOT TOLERATE RETALIATION

We can be confident in knowing that our company will not retaliate or permit retaliation if we, in good faith, report non-compliant or unethical behavior.

Here are some basics to remember:

- It is a violation of the Code of Conduct and considered misconduct to retaliate against someone for reporting a concern, in good faith.
- Retaliation will result in disciplinary action up to and including termination and, in some cases, retaliation is also against the law.
- Suspected retaliation should be reported immediately to the human resources, compliance or legal department.

Reporting in good faith means you genuinely believe the issue you are reporting is true and that you are coming forward with honest intentions, without any desire to harm others or benefit personally.



OUR ENVIRONMENT

- Maintaining a Safe Work Environment
- Human Rights
- Inclusion
- Discriminatory and Sexual Harassment
- Equal Employment Opportunity
- Soliciting and/or Distributing Literature
- Environmental Standards

MAINTAINING A SAFE WORK ENVIRONMENT

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

Here are some basics to remember:

- Disruptive behavior in the workplace or while conducting business will not be tolerated.
- Adherence to applicable drug-free workplace policies (e.g., alcohol, tobacco, substance abuse) is a condition of continued employment.
- Acts or threats of violence, harassment, intimidation, or destruction of company property will not be tolerated.
- Weapons of any type are not permitted on company premises 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 the human resources department.
- Comply with all company policies and procedures, laws and regulations affecting safety, health and environmental protection.
- Comply with all company policies and procedures affecting physical security, access control and identity management.
- Immediately report any work conditions, whether in the office, a facility or a remote location, perceived to be unsafe, unhealthy or hazardous, to the human resources or security department.



Q: A coworker has been a target of bullying by one of her peers. The behavior I observed is intimidating, and I'm afraid of also becoming a target if I speak up about the situation. What should I do?

A: Any form of intimidation (e.g., bullying) or retaliation will not be tolerated. Report the situation to your immediate manager or the human resources, compliance or legal department.

HUMAN RIGHTS

We must uphold the human rights of workers and comply with all applicable labor laws. We are prohibited from engaging in any form of human trafficking or related activities and suspicions of such should be reported immediately to the human resources, compliance or legal department. Additionally, employees may contact the Global Human Trafficking Hotline at (844) 888-Free or by email at help@befree.org.

Examples of human trafficking or related activities include, but are not limited to:

- Sex trafficking in which a commercial sex act is induced by force, fraud, or coercion;
- Recruiting, using, harboring, transporting, provisioning or obtaining a person for labor or services, through the use of force, fraud or coercion;
- Destroying, concealing, confiscating or otherwise denying access to an employee's identity or immigration documents; and/or
- Using misleading or fraudulent practices during the recruitment process or offering of employment, such as withholding information or making material misrepresentations of terms and conditions of employment.

INCLUSION

We value and benefit from the variety of experiences, thoughts, views, and backgrounds that our workforce brings. Our company values and culture emphasize how important it is to help each other be our authentic and best selves at work and to seek out different perspectives. When everyone feels like they belong, we are smarter, stronger, and better enabled to help people and communities achieve better health.

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, marital status, or any other protected class, characteristic or attribute protected under federal, state or local law. We are all responsible for promoting a work environment where everyone feels valued, respected and that they belong. Discriminatory harassment impacts our work and is prohibited.

Sexual harassment is a specific form of sex discrimination. It includes, but is not limited to, any unwelcome sexual advance, request for sexual favor, and other verbal or physical conduct of a sexual nature in any of these 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; and/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.

Refer to related harassment policies and procedures for additional information, including any applicable state or local law or regulation.

Here are some basics to remember:

- Treat fellow employees, customers, patients and others with professionalism, respect and dignity.
- Report and constructively confront all incidents of harassment.
- Do not retaliate against anyone for reporting harassment or assisting in an investigation. Retaliation 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.

Incidents of discriminatory and/or sexual harassment must be reported immediately.

EQUAL EMPLOYMENT OPPORTUNITY

It is our policy to recruit, select and hire based on qualifications for open positions and for promotion and transfer opportunities.

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, marital status, or any other protected class, characteristic or attribute protected under federal, state or local law.

We are deeply committed to attracting, developing and retaining talent and otherwise treating qualified individuals according to their ability and without discrimination.

We have a continuing obligation to hire and develop the best people we can find, basing our assessment on job-related qualifications.

Here are some basics to remember:

- All employment decisions and practices are based on job performance, experience and qualifications. This includes decisions and practices related to recruitment, hiring, training, development, compensation, benefits, promotions, transfers, corrective action, corporate-sponsored educational, social and recreational programs, and terminations.
- All levels of management are accountable for supporting the applicable company policies and procedures pertaining to equal employment opportunity.
- Employment-related discriminatory practices will not be tolerated.



Q: My department has an open position for which we are actively recruiting. I am part of the interview panel and feel that applicants are being overlooked based on their personal attributes. What should I do?

A: Our company does not tolerate discrimination of any kind. Report the situation to your immediate manager or the human resources, compliance or legal department.

SOLICITING AND/OR DISTRIBUTING LITERATURE

To prevent disruption of business activities and minimize distractions for all employees, solicitation by employees during work time or using designated work channels (e.g., email, phone, chat, virtual meetings sites) is prohibited. Distribution of literature by employees in work areas is also prohibited.

Here are some basics to remember:

- Soliciting or distributing literature by non-employees on company property or using company assets is prohibited unless a contractual agreement exists or has been approved in advance by the company to promote specific events or services.
- Do not engage in solicitation activities during work time or via work channels.
- Do not distribute literature in work areas.
- Prohibited solicitations include, but are not limited to, solicitations for political contributions, memberships in organizations, or for the purchase of merchandise or services.
- Prohibited literature distributions include, but are not limited to, political literature, product order forms, leaflets or information bulletins.
- Seek approval from the appropriate corporate social responsibility contact before soliciting for charitable contributions.



Q: Our division would like to participate in an online sports fantasy league just for fun. Is this allowed?

A: *No. Gambling is not allowed in the workplace, during company time or while using company assets.*

Q: My child's school is holding a virtual fundraiser with the funds going towards the purchase of new sporting equipment. Is it okay for me to email the fundraising link to my co-workers? After all, they can choose not to participate if they are not interested.

A: *No. Soliciting is not allowed during company time or using company assets.*

ENVIRONMENTAL STANDARDS

Our company recognizes the critical role the environment plays in the health of the communities where we live and work. We are committed to delivering health care sustainability and the advancement of programs that promote environmentally responsible practices throughout our business (e.g., minimizing waste, increasing recycling, adopting measures to save energy). We are all responsible for exercising good environmental judgment and supporting the company's standards for protecting the environment. As such, our company publicly reports and has established goals to reduce our greenhouse gas emissions.



DEALING WITH THE MARKET- PLACE AND BUSINESS PARTNERS

- Fair Dealing and Competition and Business Ventures
- Advertising and Marketing

FAIR DEALING AND COMPETITION AND BUSINESS VENTURES

We are committed to fair dealing and competition and do not engage in unfair business practices (e.g., manipulation, cover-up, concealment or the abuse of privileged or confidential information, misrepresentation of facts) or actions that illegally restrain trade or reduce competition.

Business activities must comply with federal, state, and local antitrust laws that encourage competition and prohibit certain activities limiting competition. Additionally, many of the activities that violate federal, state, or local antitrust laws may also violate federal, state, or local 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:

- Offer true and accurate information about our services or products.
- Communicate clearly so that our customers understand the terms of our business relationships, including contract performance criteria, schedules, prices and responsibilities.

- Set pricing for products and services independently, and not in consultation with any other potential provider of those products or services.
- Avoid discussing or sharing pricing or any other proprietary or confidential information with individuals who do not work for the company, especially at trade or professional meetings or events that competitors may attend. If such a discussion begins, and regardless of the setting, we should excuse ourselves immediately. An unlawful agreement involving us may end up being implied by our attendance at such discussions even if we do not participate in them.
- Avoid discussing the company's business relationships with vendors or customers with anyone not involved in those relationships.
- Clear all agreements involving exclusive relationships, preferential pricing terms or commitments not to deal with others through the compliance or legal department.
- Coordinate all merger and acquisition, joint venture and teaming arrangement discussions and agreements through the legal department.

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 providers, vendors or others that seek to insulate the company or others from competition.
- Any statements, whether oral or written, to competitors or others that could be understood to be an agreement to set prices, collude or engage in some other anti-competitive arrangement.
- Making promises that we do not believe that we will be able to keep.



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. Any time 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 the legal or compliance department.*

ADVERTISING AND MARKETING

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

All company advertising must be reviewed and approved by the marketing department or the appropriate designee. Additionally, there are special rules that apply to certain lines of business (e.g., Medicare) with which we should be familiar.

Here are some basics to remember:

- Do not make misrepresentations or misleading statements to anyone. If we make specific claims about the company's benefit plans, products or services, we must have a good faith basis for those claims.
- Plans, products or services should not be marketed in any way that might cause confusion between our plans, products or services and those of competitors. If we believe a customer or potential customer may have misunderstood us, promptly correct any misunderstanding.
- We should be alert to any situation where a competitor may attempt to mislead potential customers and inform management or the legal department of these situations.
- Do not disparage any of the products, services or employees of any competitor.



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 also arise as a result of our 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. Business is to be conducted in such a manner to avoid even the appearance of a COI in our business dealings and relationships.

The appearance of a COI can create problems regardless of the intent.

Here are some basics to remember:

- Avoid activities and situations that create a COI between personal or outside interests, including monetary interests, and the business interests of our company.
- Disclose conflicts by completing a COI disclosure form when hired, annually and when your situation changes.
- Keep your COI disclosure form updated with new disclosures as changes occur.
- Consult with the human resources, compliance or legal department 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 Dealing, Competition and Business Ventures](#) and [Dealings with Government Programs and Interactions with the Public](#) sections of this Code of Conduct.
- Seek help if there is a doubt about what may arise to a COI as it is impossible to describe all situations that may lead to a COI.



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 immediate manager or the compliance or legal department 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.*



GIFTS AND ENTERTAINMENT

- Gifts and Entertainment
- Charitable Giving and Community Investment

GIFTS AND ENTERTAINMENT

Offering or accepting business gifts or entertainment can sometimes create a perception of an inappropriate relationship or conflict of interest even if the intent is innocent and there is no influence on our business judgment.

In addition to perception, there are various circumstances in which 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.

There are certain situations in which the giving or accepting of gifts and entertainment may be acceptable on an infrequent occasion if there is no intent to inappropriately influence an individual in connection with a business transaction or decision, and the gift or entertainment is unsolicited. We may not, however, offer or accept any bribe, kickback, or other valuable consideration in connection with the sale of any of our products or services or the provision of health care services.

Refer to the applicable gift and entertainment policy for specific guidance on what is or is not acceptable. Additionally, for general guidelines to follow when dealing with government employees or officials, refer to the [Working with Government Customers](#) section.

Here are some basics to remember:

- We may accept gifts of nominal value (e.g., pens, highlighters).
- We 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 offered the waiver, reimbursement or discount.
- We may accept or provide modest meals and entertainment where the primary purpose of the meal or entertainment is business-related, or related to our duties with the company, and the expense is reasonable and customary. Also, it should not suggest a conflict of interest or improper attempt to influence business decisions, including procurement activities.

- We may not offer gifts, meals or entertainment to any government official under any circumstance. Dealing with government officials requires special attention.
- We must adhere to any more restrictive federal, state, or local laws, regulations, or rules governing gifts, gratuities, or entertainment. Consult applicable policies or procedures for additional guidance.
- We should seek help if there are any doubts about a particular situation. Contact the human resources, compliance or legal department.

Here are some situations to always avoid:

- Accepting cash or cash equivalents. If you are offered or receive cash or cash equivalents, either at home, at the office, or at a facility, tell your immediate manager right away. Return the item and inform the sender that our policy does not allow us to accept cash or cash equivalents.
- 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, refer to the [Working with Government Customers](#) section of this Code of Conduct.



Q: A vendor has offered to pay for my travel expenses so that I can attend a conference, which would otherwise be cost prohibitive for me to attend? Can I accept their offer?

A: *No. In general, accepting a vendor's offer to pay for travel expenses is not allowed. There are limited situations, however, when this is acceptable. Refer to the applicable gift and entertainment policy for specific guidance on what is or is not acceptable.*

CHARITABLE GIVING AND COMMUNITY INVESTMENT

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 activities are to be coordinated. 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, refer to the applicable corporate social responsibility and charitable giving policy, as applicable.

Here are some basics to remember:

- Be sure to forward all inquiries about community investments to the appropriate corporate social responsibility contact.
- Do not make any commitments for community investments without consulting with the appropriate corporate social responsibility contact.
- Follow all relevant company policies and procedures when volunteering as a representative of the company.



Q: Can I solicit donations (monetary or collection items) from coworkers for a personal charity or cause while I'm at work?

A: No. You are not permitted to solicit donations from coworkers while at work. Refer to the applicable corporate social responsibility and charitable giving policy for additional guidance.



ACCURATE COMPANY RECORDS AND FINANCIAL INTEGRITY

- Accurate Record Keeping
- Retention of Records

ACCURATE RECORD KEEPING

Accurate record keeping is an important aspect of doing business. In addition, certain laws and regulations require our contracts with government and other 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. Inaccuracies or discrepancies must be promptly reported to management or to the human resources or compliance department.

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. Refer to the applicable records management and retention policy and procedures for additional guidance.

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 we 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 management.

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.

Failure to maintain accurate records could result in criminal and/or civil liability, improper payments, disallowance of costs, adverse findings in judicial and quasi-judicial proceedings, inaccurate statements and false claims.



Q: I suspect that the financial report for which my coworker is accountable 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 immediate manager about it to make sure you understand the situation. You can also contact the human resources or compliance department.*

Here are some basics to remember:

- Disclose and record all company transactions. "Off-the-book" transactions are not allowed.
- Protect and regularly validate all company assets to ensure they are the same as what is 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.
- Be alert to irregularities in the way payments are made, including large cash payments and any unusual transactions and report any suspicious activity to the human resources, compliance or legal department. Our company does not condone, facilitate or support money laundering.
- Report irregularities in accounting, auditing practices or internal controls to the human resources, compliance or legal departments.
- Report any suspected fraud, waste or abuse involving our employees to the human resources, compliance or legal department.
- Report any suspected fraud, waste or abuse involving providers, patients, subscribers, agents or other persons, who are not our employees, to the special investigation unit or fraud investigation unit.

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:
 - o Making records appear as though payments were made to one person when they were made to another.
 - o Submitting expenses for reimbursement which do not accurately reflect the true nature of the expense.
 - o Falsifying time in the timekeeping system by recording time as worked when you are not working, or by working "off the clock."
 - o Changing the recipient on a claim to channel payments to an improper recipient.
 - o Deleting claims from the computer system without rerouting for reprocessing and properly documenting the action.
 - o 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 (e.g., financial statements, government programs, SOC-1 and SOC-2 audits).

**Q: I suspect my co-worker is falsifying his timesheets. What should I do?**

A: *Falsification of any company record, financial or otherwise, is prohibited. The company has programs in place to help employees when times are difficult. Talk to your immediate manager about this or contact the human resources, compliance or legal department.*

RETENTION OF RECORDS

It is good business practice to manage company 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 records must comply with all applicable records management and retention policies and procedures.



Q: Do we still have to follow records management rules while working from home?

A: *Yes. Policies and procedures related to records management and retention apply to all company records, regardless of where they are created or received.*

Here are some basics to remember:

- A record is evidence of a business transaction and/or legal obligation fulfilled, and its contents cannot be altered.
- All records regardless of storage medium or storage location, are subject to a retention period.
- Records may be in any format, such as paper, electronic, microfilm, photographs, disc, etc.
- Make sure you manage, retain and destroy all company-owned records in a manner that supports both ongoing business operations and compliance with various accounting, audit, customer, legal, regulatory and tax requirements. Refer to the applicable records management and retention policy and procedures for additional guidance.
- Follow legal hold notices issued by the legal department. Legal holds supersede records retention requirements. A legal hold notice requires preservation of applicable documents and records under special circumstances, such as pending or actual litigation, government investigation, audits or consent decrees and supersedes the requirements of the applicable records management and retention policy and procedures 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.
- Contact the records management department or the appropriate designee with any questions or concerns.

PROTECTING INFORMATION AND PROPERTY



- Cybersecurity
- Privacy
- Confidential, Proprietary and Other
Non-public Information
- Employee Data

CYBERSECURITY

As employees, we play a critical role in protecting against cyber threats. This includes being mindful of our online activities, using strong and unique passwords, and reporting any suspicious activity or security incidents immediately.

Here are some basics to remember:

- Cybersecurity is everyone's responsibility. We all help protect company systems and data by staying alert and following the rules.
- Follow company security policies and procedures. If you are unsure, ask your management or the cybersecurity team.
- Complete all assigned security training and stay informed about how to protect against cyber threats.
- Report any unusual activity, security concerns, or suspected threats to the security or IT team right away.
- Use new technology safely and only as approved by the company.
- Help support business continuity by following backup and recovery procedures when needed.
- Choose complex passwords that are not easily guessed.
- 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 okay 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 login credentials, this may be a phishing email and should be reported immediately to the cybersecurity team.*

PRIVACY

We have a legal and ethical obligation to safeguard and protect the confidential information of our customers and patients. As such, we must comply with all applicable privacy laws.

Here are some basics to remember:

- Read and comply with the applicable privacy policies and procedures and any contractual obligations that may also 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 federal, state and local 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.
- Report any known or potential breach of privacy or non-permitted use or disclosure of protected health information (PHI) to the appropriate privacy or compliance contact immediately. This includes any loss or theft of information.
- Ensure disclosure of information is only to an authorized individual or entity.
- Only use employee, member, and patient information as allowed by law, regulation or policy.
- Check for accuracy of information.
- Send all PHI securely using company approved methods.

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 to do our job.
- 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: Am I required to protect PHI for former members or are the requirements limited to just current members?**

A: *Yes, PHI of current, prior and prospective members must be protected.*

Q: I accidentally sent PHI to the wrong contracted vendor. Am I required to report this incident since it was sent to a contracted vendor?

A: *Yes. Any improper disclosure of PHI should be reported to the compliance or privacy department.*

CONFIDENTIAL, PROPRIETARY AND OTHER NON-PUBLIC INFORMATION

We must respect the sensitive nature of company confidential and proprietary information.

Confidential, proprietary and other non-public information that is obtained about our company, customers, patients 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 secret, securities and procurement laws and regulations. We 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:

- The company is assigned all rights to intellectual property that we may develop or create during our employment.
- We may not disclose or use at any time, either during or after our employment, any confidential or proprietary information gained during employment, whether or not developed by us, except as required to perform our duties as an employee of the company.
- We 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/or legal action.
- While GuideWell is not a publicly traded company, it does business with vendors that may be subject to insider trading laws.



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

A: *No. It should not be shared unless the information has been specifically designated as shareable.*

EMPLOYEE DATA

The company recognizes the importance of privacy and confidentiality regarding employee information. This includes, but is not limited to, demographic information, wage/salary data, financial/banking information, and claims/medical information.

Generally, disclosure of employee information to third parties outside the company is not allowed 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 personal insurance-related business and do not request that others in the business intervene to assist.
- When asked to provide employment references, refer the individual to the company approved verification method (e.g., automated employment verification line, dedicated verification website) or contact the human resources department for additional guidance.

Here are some situations to always avoid:

- Using employee information as test data, for training purposes or to provide examples or testimonials.
- Bypassing normal operating procedures. Any requests to do so should be reported to the human resources, compliance or legal department.

Never share employee information with other employees unless there is a business reason and it is within their designated scope of duties.



USE OF COMPANY ASSETS

- Company Assets
- Internet, Email and Social Media
- Artificial Intelligence (AI)

COMPANY ASSETS

We are responsible for ensuring that company assets are used appropriately.

Company assets include both tangible and intangible property ranging from computers, office or medical 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, storing, selling, destroying or modifying of company assets is misconduct that may result in disciplinary and/or legal action.

Examples of intellectual property include, but are not limited to, information security architecture, application source code, programs, and prototypes.

Here are some basics to remember:

- Do not use company assets for personal gain.
- Do not transfer any company asset 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 employee (other than assisting with authorized relocation expenses or emergency disaster relief efforts).
- Only use company devices, software and data for work or approved personal use.
- Do not install or use software or applications unless they are approved by the company.
- Keep company devices physically secure, especially when traveling or working remotely.
- Report incidences of lost, damaged or stolen assets to the human resources, information technology or security department.

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 that do not interfere with job responsibilities or violate the law or any company policy or procedure.

Email and internet usage is monitored to ensure compliance with policies and procedures 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 (e.g., sites that conflict with our security policies) and exceptions are not granted for personal use.

Email monitoring may result in the deletion or quarantining of any email content and delivery of an email is not guaranteed. Usage is logged, retained and monitored. Use discretion and good judgment before using company property for personal use and assume that any “personal” content is not confidential.

Here are some basics to remember:

- Be cautious with emails and messages. If something seems suspicious, do not click it, report it.
- Follow all applicable laws, regulations and company policies and procedures when using information technology resources, including the internet and the company Wi-Fi network, when using email, and when posting content on social media.
- Information technology resources, including internet and email capabilities, are provided at the sole discretion of management. Check with management if unsure about a specific department's policy.
- Exercise sound judgment when using information technology resources, including email and the internet. This also includes publishing or posting content on social media channels (e.g., Snapchat, Instagram, Facebook, LinkedIn, X, TikTok, YouTube). Refer to the applicable social media or email, internet and intranet policies for additional guidance.

Remember, we are responsible for activity performed under our login credentials and when using the company Wi-Fi network. Never share our user ID and password with anyone.

- Posting personal comments and/or views to the internet, including social media channels, must not in any way imply that the views represent the views of the company.
- Transmit PHI or other sensitive, restricted or confidential information securely using approved encryption capabilities (e.g., secure email, secure file transfer).

ARTIFICIAL INTELLIGENCE (AI)

As we increasingly integrate AI technologies into our work processes, we are committed to doing so in a responsible, transparent, and ethical manner, prioritizing the well-being of our employees, customers, and patients, while also ensuring that these technologies are used in ways that promote fairness, accountability, and respect for individual rights.

Here are some basics to remember:

- Only utilize company approved AI technologies for work purposes.
- Ensure AI utilization is reflective of our company values and ethical principles.
- Follow all laws, regulations and company policies and procedures when utilizing AI technologies, including but not limited to, data protection, privacy and non-discrimination.
- Be transparent about the use of AI technologies, including disclosing when AI systems are being utilized and providing explanations for AI-generated decisions when appropriate.
- Know the risks associated with using AI technologies and take steps to minimize them.
- Use AI technologies to inform decision-making but always involve human judgment and critical thinking in the final decision-making process.

Always verify the outputs generated by AI technologies.



Q: Can I use AI technologies found on the internet to enhance my work?

A: *No. Only company-approved AI technologies (e.g., GuideWell Chat), including those approved and provided by our authorized vendors, may be used for work purposes. Using unauthorized AI technologies can pose security risks, compromise data integrity, and create compliance issues.*



INFORMATION SECURITY

□ Information Security

INFORMATION SECURITY

The confidentiality, integrity and availability of company restricted and confidential information must be protected from unauthorized access, inappropriate use, and theft and/or loss. 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 company policies and procedures. If 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. We are required to provide access and authentication credentials prior to accessing protected information.

Here are some basics to remember:

- Correctly identify organizational information, as outlined in the applicable company policies and procedures, legal requirements, and business agreements.
- Limit sharing and use to those who need to know, and limit access based upon job role.
- Obtain appropriate approvals or authorizations and/or ensure contractual arrangements are in place before sharing information with anyone outside of the company.
- Store information according to its classification. If the classification level is not determined or is unknown, treat the information as it should be protected at the highest level of restriction until we know for certain.
- Never store restricted or confidential information on a personal mobile computing device.
- Lock your workstation when away from your desk.
- Physically secure your laptop or mobile device(s). Use extra care to protect mobile devices when traveling. Never leave mobile devices in an unlocked car.
- Respect privacy and other laws and regulations when handling sensitive, confidential or restricted information.
- Report suspected or known incidents that may impact the security or privacy of the company's information or system assets so the matter can be investigated.
- Immediately report lost, stolen or damaged computing equipment, mobile devices or media to security.
- Keep your login credentials secure and never share with others.



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 federal, state and local government entities and agencies. The laws and regulations that govern those activities are strict and often complex. Therefore, we 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 unsure about the applicable legal, regulatory or contractual requirements in a particular situation, seek guidance from the compliance or legal department. Interacting with government agencies and officials also requires a continuing commitment to the highest ethical standards, attention to detail and significant due diligence to protect the company's reputation and on-going participation in government programs.

Remember that a violation of any law or regulation can result in disciplinary action up to and including termination of employment.

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 procedures 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 the compliance or legal department activity that is believed to be unlawful, could result in a false claim, or could 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 federal, state or local government or a public entity, including a school board or a public hospital.
- Never make any form of payment, promise of payment, or give anything of value to employees or representatives of any government, company, or public or international organization for the purpose of wrongfully obtaining, retaining or directing business. Bribes, kickbacks, or other valuable considerations are prohibited under any circumstance.
- Violation of the laws and regulations regarding gifts to government employees can result in serious criminal and/or civil legal consequences.

Here are situations to always avoid:

- Deviating from contract requirements without written approval from an authorized government official.
- Offering, promising, or giving a gift, cash, or anything of value to a government employee or official.
- 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 the compliance or legal department 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 Employee Program, Medicare and Medicaid.



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 okay 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 the compliance or legal department for guidance on how to proceed with this proposed arrangement.*

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 okay?

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

POLITICAL CONTRIBUTIONS AND LOBBYING ACTIVITIES

We are encouraged to vote and be active in the political process. While doing so, it is important to know that the political process is highly regulated and there are laws that restrict individual and company political participation.

The GuideWell Political Action Committee (GPAC), our non-partisan political action committee, is one way that eligible employees may voluntarily participate in the political process. Political contributions made by GPAC are funded entirely by voluntary contributions from eligible employees. Participation is completely voluntary at the discretion of eligible employees.

Lobbying is described as a person making contact with a public official or politician regarding legislation, rules, regulations, programs and 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.

Here are some basics to remember:

- Be aware of laws, regulations and restrictions regarding political activities and contributions. Due diligence in keeping track of lobbying activities and contributions is required.
- Reimbursement is not allowed for personal political contributions, including contributions to political action committees.
- When engaging in political activities, we may do so in our individual capacity, and not as a company representative.
- Do not work on political campaigns during work hours.
- Do not use company assets (e.g., telephones, copy machines, email, internet) as part of a campaign effort, including fundraising.
- Seek guidance from the applicable government relations department before agreeing to do anything that could be construed as involving the company in any political activity.

Lobbying disclosure laws require the reporting of contacts with public officials or politicians and expenses and include activities beyond promoting or opposing legislation.

Here are some situations to always avoid:

- Soliciting political contributions on company property. (Our GPAC may solicit eligible employees on company property during work time.)
- Distribution of literature on company property or use of company assets for political purposes.

**Q: I am a volunteer for a political candidate. Is this okay?**

A: Yes. It is okay as long as your activities are performed 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 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 or may require prior approval for it to occur. Offshoring generally 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 for which you are working. Check with the compliance or legal department immediately if you become aware of offshore activities involving our State Group, Federal Employee Program, Medicare Advantage, or Medicaid business.



Q: I recently discovered that a vendor we use is offshoring translation services. Is this okay since the translation services represents only a small volume of work that the vendor performs on our behalf?

A: *No. Offshoring of services may not be permitted or may require prior approval for it to occur. Check with the compliance or legal department immediately if you become aware of offshoring activities..*



LEGAL AND REGULATORY REQUIREMENTS

- Legal and Regulatory Requirements

LEGAL AND REGULATORY REQUIREMENTS

We are subject to many federal, state and, in some cases, even local laws and regulations that apply to our business. Although not inclusive and all are not mentioned in the Code of Conduct, the following are some of the laws with which we 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 the compliance or legal department.

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 their 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.

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.

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 Statute 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 law 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 Statute (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 their family) has an ownership or investment interest or with which they have 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 plans include certain essential health benefits, and the availability of cost sharing subsidies and premium tax credits, among numerous other provisions (certain reforms do not apply to Puerto Rico).

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.

Telephone Consumer Protection Act (TCPA)

The 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.

RESOURCES

We are not expected to have the answer to every compliance or ethics question, but we are expected to know when to ask for help and where to go for help. Below are several resources available to assist us:

FLORIDA BLUE	
Report a compliance or ethics matter	<p>Immediate manager, as applicable Helpline: (800) 477-3736 ext. 56300 File an online report: www.compass.ethicspoint.com Email: compass@guidewell.com QR Code:</p>  <p> SCAN ME</p> <p>Chief Integrity, Compliance and Risk Officer: (904) 905-5068 Director, Business Ethics: (904) 905-4264 Human Resources (Employee Relations): (904) 905-4995 Legal Affairs: (904) 905-6768</p>

FLORIDA BLUE	
Privacy	Privacy Helpline: (888) 574-2583
Security	<p>Non-emergency incident: (904) 905-2009</p> <p>File an online report: https://floridablue.omnigo.one/CESIReportExec/OLR/OLRMain.aspx?IsAuth=1&groupid=103</p> <p>Email: security@guidewell.com</p> <p>QR Code:</p>  <p></p>
Special Investigation Unit	<p>Phone: (800) 678-8355</p> <p>Fax: (904) 905-5925</p> <p>Email: specinvestunit@floridablue.com</p> <p>Complete a Fraud and Abuse Report at: floridablue.com or the Intranet at: http://cag.bcbsfl.com/sites/beic/SIU/default.aspx</p> <p>Mail: Florida Blue, Special Investigation Unit P.O. Box 44193 Jacksonville, FL 32231-4193</p>
Company Policies	http://cpol.bcbsfl.com/Pages/Home.aspx
HR Policies	http://hr.bcbsfl.com/Pages/HRPolicyView.aspx

TRIPLE-S MANAGEMENT CORPORATION	
Report a compliance or ethics matter	Immediate manager, as applicable Helpline: (866) 384-4277 File an online report: www.ethicspoint.com
Audit and Risk Committee	Mail: Attention - Audit and Risk Committee P.O. Box 363628 San Juan, PR 00936-3628
Internal Audit Office	Phone: (787) 277-6076 Mail: Attention - Internal Audit Office P.O. Box 363628 San Juan, PR 00936-3628
Legal Affairs Office	Phone: (787) 749-4949 ext. 8321948 Mail: Attention - Legal Affairs Office P.O. Box 363628 San Juan, PR 00936-3628
Triple-S Propiedad and Triple-S Insurance Agency	Phone: (787) 749-4600 ext. 8321869 Compliance Office Email: cumplimentosp@ssspr.com Special Investigation Unit Email: siutsp@ssspr.com Mail: Attention - Compliance Office P.O. Box 70313 San Juan, PR 00936-8313
Triple-S Salud and Triple-S Advantage	Phone: (787) 749-4949 ext.8322438 Compliance and Privacy Email: TSACompliance@ssspr.com Special Investigation Unit Email: fraude@ssspr.com Mail: Attention - Compliance Department P.O. Box 363628 San Juan, PR 00936-3628
Triple-S Salus Quality and Compliance Office	Email: saluscompliance@saluspr.com Mail: Attention - Quality and Compliance Office PMB 509 P.O. Box 7891 Guaynabo, PR 00970-7891
Triple-S Vida	Phone: (787) 777-8432 ext. 8351730 Compliance Office and Special Investigation Unit Email: cumplimiento@sssvida.com Mail: Attention - Compliance Office P.O. Box 363786 San Juan, PR 00936-3786
Triple-S HR Policies - located in employee portal (intranet) Triple-S Salud and Triple-S Advantage Policies - located in Compliance 360	

WEBTPA/COMMUNITAS	
Report a compliance or ethics matter	<p>Immediate manager, as applicable</p> <p>WebTPA Compliance Line: (800) 371-2919</p> <p>Communitas Compliance Line: (800) 371-2919</p> <p>File an online report: www.webtpa.com/compliance-and-ethics</p> <p>Director of Compliance: (469) 417-1894</p> <p>Senior Manager, Human Resources: (469) 417-1663</p>

FLORIDA HEALTH CARE PLANS (FHCP)	
Report a compliance or ethics matter	<p>Immediate manager, as applicable</p> <p>Helpline: (386) 615-4080, or ext. 4080 internally</p> <p>File an online report: compliance@fhcp.com</p> <p>FHCP Compliance and Privacy Officer: (386) 676-7105</p> <p>FHCP Human Resources (Employee Relations): (386) 676-7153</p>
Privacy	<p>Privacy Helpline: (386) 615-4080 or</p> <p>FHCP Compliance and Privacy Auditor: (386) 615-4088</p> <p>FHCP Compliance and Privacy Officer: (386) 676-7105</p>
Fraud Investigation Unit	<p>Phone:</p> <p>FHCP Compliance and Privacy Officer: (386) 676-7105</p> <p>FHCP Compliance and Privacy Auditor: (386) 615-4088</p> <p>Email: compliance@fhcp.com</p> <p>Mail: FHCP Compliance Department</p> <p>Fraud Investigation Unit</p> <p>2450 Mason Ave.</p> <p>Daytona Beach, FL 32114</p>
Company Policies	FHCP's Company Policies are located in PolicyTech
HR Policies	FHCP's HR Employee Handbook/Policies are located in PolicyTech

GUIDEWELL

GuideWell Mutual Holding Corporation