



GHX Global Code of Conduct

September 2024



Table of Contents

Letter from the CEO	3	Government Customers and Contracting	13	Records Management	24
Introduction	4	Event Registration and Travel	13	Employment and the Workplace Environment	25
Culture of Compliance	4	Political Activity	13	Hiring and Contracting	26
Code of Conduct	5	Fair Dealing and Competition/Antitrust	14	Selection and Use of Third Parties	27
GHX Business	6	Import and Export Compliance	15	Non-Discrimination and Anti-Harassment	27
Internal Processes	7	Preventing Money Laundering and Terrorism Financing	15	Committed to Human Rights	27
In General	7	Ethical Decision-Making Decision Guide	17	Physical Safety and Health	28
Contracting	7	GHX Resources	18	Reporting and Investigations	29
Product Offerings	7	In General	19	Effective Lines of Communication & Reporting	30
External Communications	8	Information Technology Resources	20	Duty to Report	30
Intellectual Property of Others	9	Confidential Information	20	Where to Report	31
Fraud and False Statements	9	Protecting Confidential Information	20	Non-Retaliation	32
In General	9	Data Privacy Laws	21	Investigations & Response	33
Honesty in Recordkeeping	9	Exchange and Receipt of Confidential Information	22	Investigations	33
Conflicts of Interest	10	Competitors' Confidential Information	23	Enforcement & Disciplinary Action	34
Insider Trading	11	Reporting Breaches of Confidentiality and Security	23	Disciplinary Action	34
Anticorruption	12	Disclosing Trade Secrets in Whistleblower and Retaliation Claims (U.S. Only)	23	Corrective Action	34
Gifts and Entertainment	12	Social Media	24	Change Control Grid	35
Bribes and Kickbacks	12				



Letter from the CEO

Our company was founded on doing the right thing. We have never shied away from challenges and tough decisions if we believed the outcome would create a positive, lasting impact on everyone in the healthcare ecosystem. Because of our mission-driven culture, GHX has built a reputation as a trustworthy market leader over the past 24 years.

Maintaining that trust requires us to hold ourselves to exceedingly high standards. That means consistently demonstrating ethical behavior with one another and to our customers, in service to the patients and families we serve together. By staying true to our core values (Collaborate, Innovate, Inspire and Grow), GHX's Code of Conduct is more than a policy – it's a continuous commitment to our company's origins.

As we aspire to expand our impact and deliver \$30 billion in savings to the global healthcare industry by 2027, our Code of Conduct will serve as a guidepost for how we grow, make decisions and comply with applicable legal and ethical standards. Ultimately, we believe our Code will deliver on our mission and vision of ***simplifying the patient-centered business of healthcare to improve outcomes as to create a future where affordable, quality care is possible for all.***

The vitality of our culture of compliance depends on every member of the GHX workforce understanding and adhering to this Code of Conduct each day. I ask that you do more than simply read this Code of Conduct. I want you to take the time to process it and consider how the daily actions you take can serve to further strengthen it in service of our mission.

And I welcome your feedback on how we can continue to improve our compliance program in the interest of our colleagues, our customers and our business partners.

If ever you are faced with an ethical or compliance dilemma, raise your concerns as described in the Reporting and Investigations section of this Code of Conduct. Keep the lines of communication open, escalate risks promptly and resolve conflicts constructively and with respect. Everyone at GHX should feel confident that they are working with colleagues who value and act with integrity.

Thank you for your dedication to weaving the principles of our Code of Conduct in our cultural fabric. In doing so, we will continue to honor our legacy of doing the right thing for the benefit of all.

Sincerely,

Tina Murphy

Culture of Compliance

The policy of Global Healthcare Exchange, LLC and its subsidiaries worldwide (“GHX” or the “Company”) is to comply with applicable laws and ethical standards. Compliance is a key part of GHX’s corporate culture and essential to our business. Maintaining a robust corporate compliance program positions GHX to successfully operate in a compliant, ethical manner. Federal and state government agencies also assess and enforce compliance, and implementation of a corporate compliance program is an important step in proactively addressing the government’s enforcement efforts. This means that all Company directors, officers, employees, temporary agency staff and other contractors, and agents (“Personnel”) have responsibility for:



understanding the legal and ethical standards that apply to their work;



meeting those standards in their work;



asking questions when they do not understand;



promptly reporting noncompliance; and



not engaging in or tolerating any form of retaliation against anyone who reports potential violations in good faith.

As part of GHX’s Compliance Program, this Code of Conduct defines the types of behavior that GHX expects of its employees, officers, volunteers, contractors, and vendors (individually and collectively “Personnel”) in light of its accountability to our customers, the government and other payors, and our fellow coworkers. The Code of Conduct details the fundamental principles, values, and framework for action within the organization, contains the basic legal principles under which GHX must operate, and explains how Personnel should respond to violations of the Code of Conduct.

GHX’s Corporate Compliance Program is comprised of this Code of Conduct and underlying policies and procedures. Such policies, procedures, and practices apply to the conduct of Personnel in their day-to-day operations. The policies and procedures are developed under the direction and supervision of the compliance officer, compliance committee, and operational managers. They are distributed to affected Personnel, and Personnel are required to comply with such policies and procedures.

Code of Conduct

This Code of Conduct describes behavior that we expect of our Personnel. This Code of Conduct does not detail all legal and ethical requirements that apply to you and cannot hope to cover every issue that may arise. If you have questions, ask the Compliance or Legal Department.

The Company has also adopted policies and procedures that provide more detail around legal and ethical requirements. The requirements may vary by work role and location. The Company updates its policies and procedures from time to time, so make sure you are familiar with the current versions that apply to you. Any deviation from official Company policy requires prior approval by the Compliance or Legal Department.

To help you understand our requirements, you must periodically complete GHX compliance training and certify to certain key requirements.

The Code of Conduct does not create or modify any type of contract or agreement. It also does not limit or alter any other Company policy or applicable law. You should be aware that activity of members of your family, household, and significant others may create conflicts of interest and affect your responsibilities.

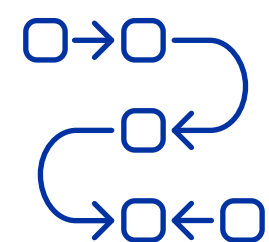


GHX Business

The Company's corporate reputation depends on you performing your work with honesty and integrity, in line with our core value, Inspire. The following sections describe some key areas where integrity matters to our business.



Internal Processes



In General

Where the Company has established processes, you must follow them. Many GHX processes are designed to include important compliance controls, such as preventing fraud, and some of those may not be obvious to you. Internal processes are also important for GHX's core value, Collaborate. If you aren't sure about the process for doing something, ask your manager or the Compliance Department. If you feel a process could be improved, we encourage you to speak up and help make it better, in line with our core value, Innovate.



Contracting

GHX uses standardized processes for the negotiation and execution of contracts with customers, vendors, and our Personnel. The Company also has formal purchasing processes. These standardized processes cover new agreements, renewals, and changes to existing agreements or spending. They help us collaborate to standardize our product offerings, meet our obligations, prevent fraud and waste, and reduce legal liability. You must comply with these requirements, including using approved forms and obtaining prior legal review and spending approvals where required. GHX has very few authorized signatories, and so most Personnel are not authorized to sign contracts on behalf of GHX, including orders, quotes, and electronic or online click-through agreements. If you receive something asking for your signature, check with Legal first.

If you have questions about customer contracting, please ask Contract Operations. Questions about vendor spending or contracting should be directed to Procurement.



Product Offerings

We are dedicated to quality and take personal pride in all the products and services we provide. Our focus on the needs of our customers continuously drives us to improve. Our continued success depends on meeting or exceeding our customers' expectations, and standing behind everything we do. Innovating our products can involve complex issues of data rights, intellectual property, and data privacy and security, among others.

As a reminder, the Legal Department needs to be engaged early in the process for designing, developing, or changing any product, to allow them enough time and information to identify and address issues.



External Communications

In order to have the Company speak in a unified voice (in line with our core value, Collaborate), Corporate Communications is responsible for all external Company communications. You should not make any public statement on behalf of the Company or respond to requests for information from outsiders, including the media, unless you are authorized to do so. Even if authorized, you must confer with Corporate Communications and the Legal Department.

The Legal Department must preapprove the following content:

- advertising, sales, and marketing materials;
- mass emails to customers or potential customers;
- presentations to customers and other external parties (including industry analysts);
- other public statements and representations (e.g., media statements, press releases); and
- any language to be posted on the Company's external websites.

You must get advance approval from Product Marketing for all product-related sales and marketing materials. You will also need to coordinate in advance with Corporate Communications for any endorsement or promotion of any third-party entity, product, or event in the name of the Company and any vendor or partner use of Company names and logos.

It is important that any communications with customers or third parties about operational, security, or privacy events be accurate and coordinated. Please contact Customer Support regarding any customer-facing operational event, and the Security and Compliance Teams regarding communications about any security or privacy events.

Intellectual Property of Others

You must obtain and comply with all licenses, permits, and approvals required under all applicable laws. Comply with all product licenses and avoid obtaining, reproducing, distributing, or altering copyrighted or licensed materials in violation of those rights. You may not use photos, videos, audio, graphics, computer software, logos, training slides, presentations, articles, or other materials in your work in a way that violates intellectual property laws of any jurisdiction. You may not acquire or install non-licensed computer software and may not illegally copy software licensed by the Company for use by any individual, the Company, customers, consultants, or any other third party.

Fraud and False Statements

In General

We expect you to be truthful in your work. You must avoid knowingly making materially false oral or written statements or omissions to the Company, our customers, governmental entities, and others. This means being honest about who you are, what your position is, and what you are doing in your interactions with others. If business can only be obtained by improper or illegal means, the Company's policy is to forego it.

All sales and promotional efforts must be free from deliberate misrepresentation. If GHX cannot meet a commitment to a customer, you should work proactively with internal teams and the customer to address the problem (Collaborate).

You may not misrepresent yourself or your situation (e.g., by posing as someone else) to get information or access. You may not seek or obtain competitive intelligence through deception, theft, illegal entry, illegal computer access, or electronic eavesdropping. You must not mislead anyone about our competitors or their operations.

Honesty in Recordkeeping

The Company relies on the accuracy and completeness of our business records. You may not create false or misleading records or entries, or alter, destroy, or hide data to make records false or misleading. The Company requires that:

- you accurately report financial and operational information as required by your work;
- you do not take or authorize any action that would intentionally cause the Company's financial records to fail to comply with applicable law, policy, or generally accepted accounting principles;
- any record that may support any payment or reimbursement be complete, honest, accurate, and appropriately documented (e.g., time sheets, expense reports, insurance claims, or records that a customer may use to obtain government reimbursement programs (such as Medicare or Medicaid in the U.S.));

- you do not cause Company records to be intentionally misleading about the nature of any transaction;
- no cash or other assets be maintained for any purpose in any unrecorded or “off-the-books” fund; and
- you report any financial or operational irregularities in a timely manner to the Company, as described in “Reporting and Investigations” [on page 29](#).

Conflicts of Interest

You must disclose to the Company any conflicts between the interests of the Company and you, your significant other, or immediate family members of you or your significant other. A conflict of interest arises when your activities (or those of your family or significant other) conflict, or appear to conflict, with your ability to serve the best interests of the Company or to perform your work objectively and effectively. Examples include:

- having a leadership, consulting, or employment position or direct financial interest in a Company competitor or vendor;
- using your Company position to advance your own financial interests or your family’s or significant other’s;
- directing business to a vendor or service provider owned or managed by you, a family member, or significant other;
- being self-employed in competition with the Company;

- accepting or soliciting anything from a vendor that might compromise or appear to compromise a Company decision maker’s objective assessment of the vendor’s product or price;
- accepting cash, gifts, entertainment, or benefits that violate the Company’s Anticorruption Policy, as described [on page 12](#) in “Anticorruption;” and
- having a relationship or interest that interferes with the ability of anyone to conduct their work.

The Company may allow you to hold outside employment or self-employment that doesn’t compete with us, compromise our interests, use our resources (including office space, computers, phones, supplies, or intellectual property), violate our policies or agreements, or interfere with anyone’s work for the Company. You may not work through a temporary agency in a second job for the Company, including a different subsidiary. Please refer to your local Employee Handbook or your employment contract.

Example

Your brother’s company offers the perfect solution to a GHX need.

You must notify the Compliance Department before you engage that company, and you must follow any restrictions. For example, you may need to obtain bids from other companies and recuse yourself from any decisions involving your brother’s company.

If you learn about an opportunity through your GHX work or GHX resources, you may not take personal advantage of it without prior authorization from the Compliance Department, Legal Department or Board of Directors. Even if you learn about an opportunity outside of GHX, it may represent a conflict of interest if it relates to the Company's existing or contemplated lines of business.

If you aren't sure whether a conflict of interest may exist, you must review the situation with the Company's Legal Department. No actual, apparent, or potential conflict of interest may be waived or ignored without the prior approval of the Company's Compliance Department. Failure to disclose a conflict of interest to the Company may result in disciplinary action.



Insider Trading

In your work, you may learn non-public information about GHX or other companies' business. Although the Company is not publicly traded, many of our customers are. You are prohibited from using any material, non-public information to buy or sell securities or for other personal gain. You are also forbidden to share such information with others, except as necessary to conduct Company business and in compliance with our policies and agreements.

"Material" information is anything that a reasonable investor would consider important in deciding to buy, sell, or hold securities. A few examples are:

- new products, processes, or initiatives;
- acquisitions or divestitures of businesses, product lines, or technology;
- earnings figures and trends or other corporate financial information;
- important litigation, negotiations, contract, or joint venture information; and
- imminent regulatory or other government action.

Confidential information is considered non-public until an official announcement has been widely distributed and investors have had an opportunity to evaluate the information. Violations of these insider trading rules may result not only in disciplinary action by the Company, but in criminal prosecution and/or civil penalties. If you have any questions about policies on insider trading, including whether information is "material" or "non-public," consult the Company's Legal Department.

Anticorruption

The Company is subject to overlapping anticorruption laws worldwide. Law enforcement authorities in many countries have been aggressively enforcing anticorruption laws, particularly in the healthcare industry. The financial and criminal penalties imposed on individuals and companies can be significant. You must adhere to the Company's Anticorruption Policy located on the Compliance and Legal Hub page and work closely with the Compliance Department to resolve any related issues.

Gifts and Entertainment

Giving or receiving gifts or entertainment can create conflicts of interest and violate laws or ethical standards aimed at preventing corruption or unfair business practices. Gifts and entertainment are not appropriate if they create any kind of obligation or the appearance of bias or are given with the intent to gain an improper advantage with customers or vendors or to facilitate approvals from government officials. You may not solicit or accept any gifts or entertainment that might influence or appear to influence your decisions on behalf of the Company, or that might be viewed as additional payment above your compensation by the Company. You are not allowed to personally benefit from the Company's purchase of goods or services from a company or supplier. Never accept cash, checks, money orders and/or gift cards. Any gifts, entertainment, travel, and other things exchanged during the course of Company business should be:

- of nominal value of no more than \$15 from a single source and \$50 from all sources in a year;
- connected and proportional to a proper business need;
- customary;
- permitted by applicable law and policy on both sides;
- not intended for any improper purpose; and
- if submitted for payment or reimbursement as an expense, accurately documented in Company records.

When working with public officials, you must be aware that even simple offers, such as purchasing a meal or refreshments, may be unacceptable or even illegal. You must contact the Compliance or Legal Department before providing any gift or entertainment to a public official.

Keep in mind that our customers and others may be subject to different laws and policies, some of which may be much stricter. If you intend to give a gift or entertain someone, you should first check if they are allowed to accept it.

Bribes and Kickbacks

You must not offer, give, solicit, accept, or receive any form of bribe, kickback, or inducement. This applies worldwide, even where the practice is common or accepted. To help prevent our vendors, consultants, agents, or representatives from

offering or receiving bribes or kickbacks, all arrangements with such entities must be reduced to written contract, approved by the Company's Compliance Department, and documented in accordance with applicable law, accounting requirements, and ethical business practices. All payments and other items of value given to such entities must be accurately, completely, and honestly reflected in the contract and Company financial records, and be in line with the activities undertaken.

Bribes: A bribe involves giving or receiving anything of value to influence someone to do something other than carrying out their official duties in an impartial manner. Merely offering to give or receive a bribe is a violation, even if no exchange is ever made. Anything of value includes not only cash, but also, for example, gifts, entertainment, travel, discounts, education, sponsorship, speaking or consultation fees, home improvements, promises of employment, or charitable or political donations.

Kickback: Kickbacks involve improperly returning a portion of earnings or giving gifts as a reward for the other party's actions in making the earnings possible. Prosecution of kickback schemes is common in healthcare, including for improper gifts, travel, entertainment, speaking fees, and free samples for promoting certain products.

Government Customers and Contracting

When doing business with federal, state, or local governments, all statements and representations to government procurement officials must be accurate and truthful, including costs and other financial data. If your role involves direct interaction with government or supervision of someone in such a role, you must know and follow the applicable special government rules and regulations and avoid any conduct that could even appear to be improper. Payments, gifts, or

other favors given to government officials or employees are strictly prohibited, and Personnel must follow the Company's Travel and Entertainment and Anticorruption Policies. Violation may expose the Company and our government customers to substantial fines and penalties.

Event Registration and Travel

Any offer to compensate non-GHX personnel for registration fees and travel expenses ("comps") to a Company event, including the GHX Summit, must comply with this Code of Conduct and other Company policies and requirements to avoid creating even the appearance of improper influence. The GHX Summit is an important business event bringing together customers and others to learn about and discuss common industry issues. Comps should be offered to entities that will get value from, and contribute to, the educational and networking benefits of the event. They are not gifts or entertainment for individuals. If you want to offer comps to a government customer, or to a customer in the current sales cycle, you'll need to first obtain Global Leadership Team approval through the standard deal desk process. You must confirm that any intended recipient is not prohibited from accepting comps by applicable law or their employer's policies.

Political Activity

The Company respects your rights to engage in political activity. However, these activities should never be conducted on Company time or using Company assets (including office space, computers, telephones, cell phones, supplies, or intellectual property) without the prior approval of the Board of Directors. Political activities

should always be separated from your relationship with the Company, should not convey the impression that your political views are shared by the Company, should not create the appearance of impropriety, and should always comply with applicable law. You may not commit the Company to making a political contribution without prior approval from the Board of Directors. You are also prohibited from soliciting political contributions from persons with whom the Company does business without the Board of Directors' prior approval. You must promptly notify the Company's Compliance Department if you, an immediate family member, or your significant other has been elected or appointed to any political office or government-related position, whether paid or unpaid, domestic or foreign.

Fair Dealing and Competition/Antitrust

Fair competition laws, including antitrust laws, limit the ways the Company can conduct itself in the marketplace. These laws are complex, and our trusted industry position makes it particularly important for you to observe the principles of free and fair competition. You must comply with applicable antitrust laws, regulations, and Company policy and not engage in price fixing, collusive bidding, or purchase tying arrangements. Failure to comply with applicable antitrust laws can lead to criminal prosecution and fines for companies as well as individuals, and to jail terms for individuals. Many entities with which we do business, including our customers, suppliers, and competitors, are competitors with each other and have customer-supplier relationships with each other. You must be careful that Company activities do not facilitate collusion or create the appearance of collusion.

Even practices not involving competitors may violate antitrust and competition laws, depending on business justification and effect on competition. For example:

- Exclusive dealing
- Bundling/package offerings
- Resale restrictions
- Selective discounting

You should contact the Legal Department with any questions about the legality of practices or conduct under the antitrust and competition laws. If you become aware of any potential violations, contact the Legal Department or report through the Compliance and Ethics Hotline or appropriate toll-free number as described under 'Where to Report' [on page 31](#).

Example

You plan to hold a meeting of supplier customers to discuss industry trends and solutions.

You should make sure a GHX attorney can attend to help monitor and steer the discussion to prevent even the appearance of anticompetitive collusion. You will also need to review and distribute the Company's standard Antitrust Guidelines at the start of the meeting.

Import and Export Compliance

You are required to comply with applicable import and export laws of countries and international organizations. These laws vary by location and activity. Keep in mind that allowing someone from another country to access data or source code electronically can be deemed an export to that person's home country, regardless of where that person, data, or source code are actually located. Laws in a number of countries prohibit directly or indirectly doing business with certain sanctioned countries, entities, and individuals. In addition, some technology is subject to export restrictions and licensing requirements. The Company's Legal Department must approve in advance any significant international Company investment or transaction.

Preventing Money Laundering and Terrorism Financing

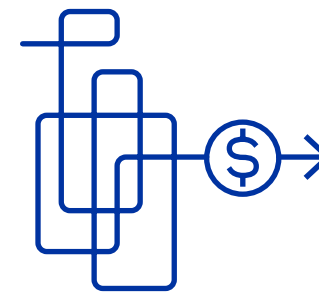
Money laundering and terrorism financing are serious global problems and are prohibited by U.S. and other applicable laws. Money laundering is the process of making illegal proceeds appear legitimate. Note that this practice is not limited to cash transactions. Complex commercial transactions may hide financing for criminal activity such as terrorism, illegal narcotics trade, bribery, and fraud. The Company prohibits knowingly engaging in transactions that facilitate money laundering or result in unlawful diversion, and has a policy of conducting only legitimate business with reputable customers and vendors.



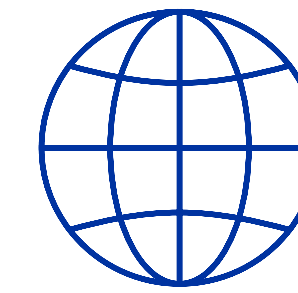
Watch for and report the following red flags:



Requests for cash payment, traveler's checks, or checks from an unknown third party



Unusually complex payment patterns or deal structures



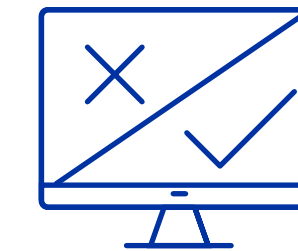
Unusual transfers involving countries not related to the transaction



Customers, vendors, or third parties who seem eager to avoid recordkeeping requirements

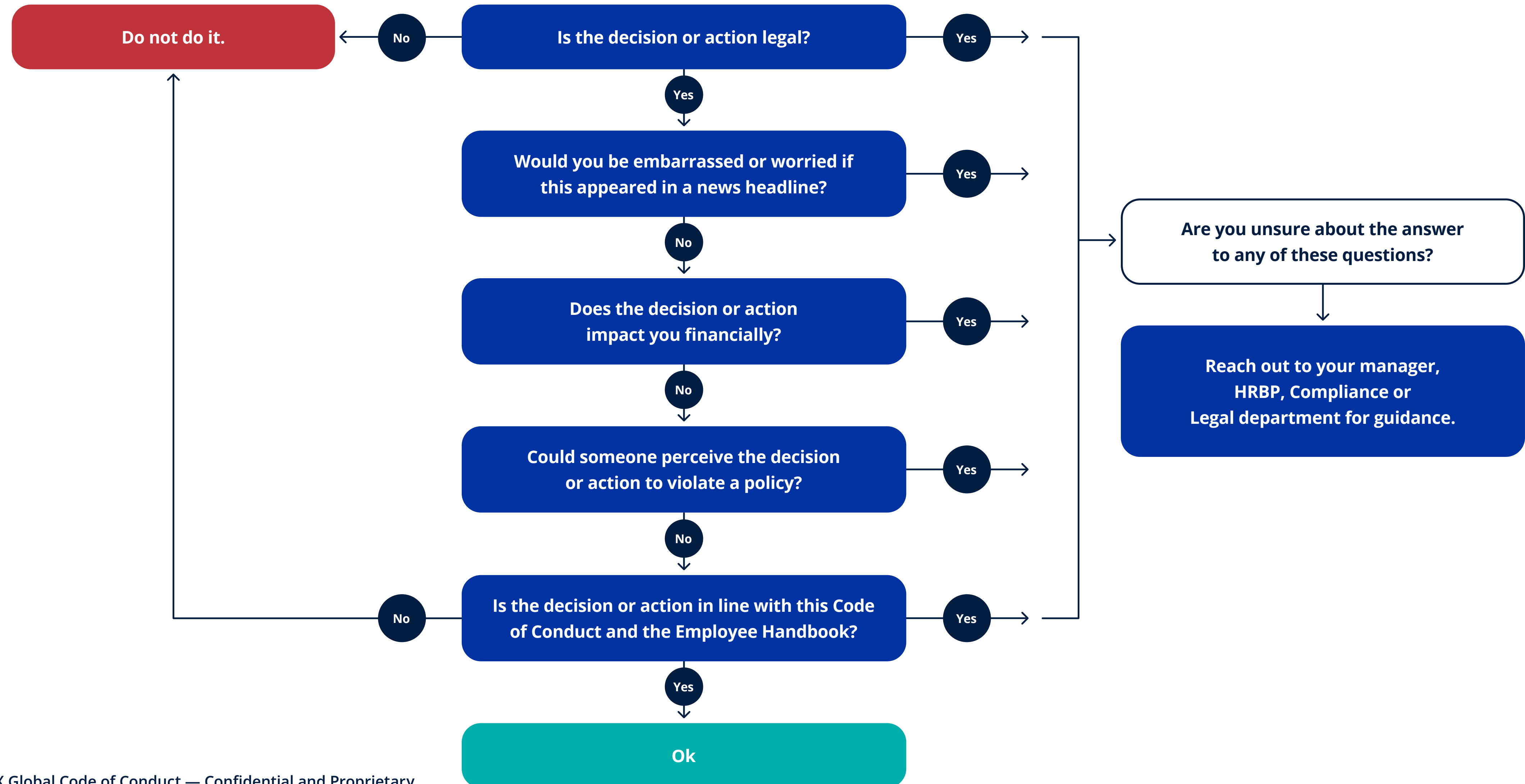


Transactions involving locations previously associated with money laundering or tax evasion



Transactions that are inconsistent with usual business practices or an entity's normal pattern of activity

Ethical Decision-Making Guide



GHX Resources



In General

Our core value, Grow, depends on efficiently using our assets. Theft, waste, and loss directly impact our profitability and, ultimately, all our jobs. You must protect all Company property entrusted to you, use it properly, maintain it in good condition, and return it to the Company when you stop working for us.

All supplies, equipment, services, utilities, and other resources the Company buys should be used only for legitimate Company business. The Company may permit some incidental personal use of Company resources (such as limited personal telephone calls or Internet use), so long as it does not interfere with anyone's work or Company business; is not for personal gain, for the benefit of another business, for political advocacy, or for any improper or illegal purpose; and does not otherwise violate this Code of Conduct or other policy, including the Employee Handbook for your jurisdiction. Any personal use of Company resources does not make them your own. Unless applicable law requires otherwise, you should not expect that any communication or data using Company resources will remain private, even if password-protected or stored externally. To the extent permitted by applicable law, Company management may access such communications, data, and resources and may also allow law enforcement authorities or other third parties to access it.

You may not use Company names, logos, brand names, trademarks, or letterhead for personal purposes. Using Company facilities or property for purposes other than Company business (e.g., after-hours use of rooms for charitable or other groups) is prohibited except with the prior written approval of the Company's Compliance Department.



Information Technology Resources

Our business depends on our information technology (“IT”) resources remaining continuously operational and accessible to Personnel and customers. Access to confidential information must be restricted to authorized users. You must always maintain the physical and operational security of these Company resources, including Company email and software accessed through a personal mobile device in compliance with the GHX Corporate IT Policy. The Company maintains several policies and procedures detailing its IT operations and enterprise information security program. Among other things, these:

- require you to protect Company IT resources and data from theft, loss, compromise, and damage;
- provide controls over the access of users and technology to Company IT resources and data;
- prohibit use of Company IT resources for illegal or improper purposes;
- require you to report any security, privacy, or operational issues immediately; and
- require you to return any GHX devices to the Company when your relationship with GHX ends.

Confidential Information

One of the Company’s most important assets is information. Proprietary Company information, such as business plans and technical data, must be protected to avoid loss of business or competitive advantage. Information that belongs to customers or third parties must be protected to avoid loss of trust or liability for damages. Some information is protected by law and must be kept confidential to avoid legal liability.

The Company requires you to comply with broadly defined confidentiality requirements. This section of the Code of Conduct highlights a few of these requirements. You should refer to the applicable Employee Handbook and/or employment contract for further details.

Protecting Confidential Information

You should make a conscious effort to protect confidential information in whatever form it takes, including written documents, digital files, conversations, and photos.

Mark confidential or proprietary materials as such. Company confidential information should never be stored in any unsecure place or any personal device or service (e.g., cloud sharing applications not authorized by GHX IT, flash or thumb drives, etc.). You must take extra care in transmitting confidential information in any manner that may increase the chances of unauthorized access, including faxes, email, and voice mail.

You should be very careful about discussing Company business in public, including in restaurants, on elevators, on airplanes or in airports, on the telephone or wireless networks in public settings, and at customers’ facilities. Unless authorized

by Corporate Communications, you should not discuss Company business on the Internet or social media, whether or not you use your real name. You should not disclose confidential information to other individuals who do not have authority or a legitimate business need for it, including by leaving confidential information in a place where it can be easily viewed by or accessible to others (e.g., on your desk, on a copier, in a meeting room, or in unrestricted digital folders or sites).

Dispose of materials that contain confidential information in a way that prevents disclosure (i.e., by sanitizing electronic media and placing documents in the secure disposal bins at Company facilities). When disposing of equipment that stores confidential information in electronic form, you must be sure that any memory storage devices (e.g., hard drives, back-up media) are thoroughly wiped according to Company standards. As more equipment becomes computerized and connected to the Internet, be aware that confidential information may be stored or transmitted where you may not expect it. Be especially careful when disposing of information that could be used to identify or trace any person and any equipment on which such information may be stored. Consult with the Compliance Department about any disposal questions.

Data Privacy Laws

We take data privacy seriously, and we expect you to do the same. You must protect any information that can be linked to an individual person, whether that person is a patient, a Company employee or contractor, a customer representative, or someone else. Examples of information that can be linked to an individual or considered personal data is their name, date of birth, social security number/

national identification number, address, personal or business email address, medical record number, employee number, etc. Sometimes, the best way to protect personal data may be not to receive it in the first place. Data protection laws and regulations are rapidly developing around the world and include the Health Insurance Portability and Accountability Act (HIPAA), the Canadian Personal Information Protection and Electronics Documents Act (PIPEDA), the European Union General Data Protection Regulation (GDPR) and similar European country laws, the California Consumer Privacy Act (CCPA), and others. The Company maintains policies to help us comply with this complex network of laws and regulations, and you must learn and follow their requirements. Please consult with the Compliance Department if you have questions.

Example

You are designing a new product and deciding what data fields are needed.

Consider carefully whether data that may be traced to an individual person is necessary, including lot and serial number of devices implanted in a patient.

Exchange and Receipt of Confidential Information

Do not disclose any Company confidential information to any third party or receive confidential information from a third party unless and until a non-disclosure agreement approved by the Legal Department is fully executed by authorized signatories. If you share Company confidential information verbally, you should specify at the outset that the information is confidential and is subject to a non-disclosure agreement that is in effect at that time. Certain types of confidential information such as patient data or other personal data may require additional contracting, as discussed in the Company Information Classification and Handling Guidelines. Consult the Legal Department if you may need a non-disclosure agreement or additional guidance on this issue.

You should be aware of the risks associated with receiving other parties' confidential information. These include the risk of lawsuits for unauthorized use or disclosure of such information, including allegations of intellectual property infringement, that could result in significant damages, royalty payments, or being barred from selling certain products or services. You may not receive information of others that is marked as confidential or that they have reason to believe may be confidential without first consulting with the Company's Legal Department about the associated business and legal risks. If you receive confidential information from a third party, you must restrict access to that information as required by the confidentiality agreement and avoid any allegation of unauthorized use.



Competitors' Confidential Information

You must not improperly gain access to, utilize, or disseminate any confidential commercial information belonging to competitors. You are prohibited from interviewing or engaging anyone to gain improper access to that person's current or former employer's trade secrets. It is also unacceptable to put anyone in a position that would pressure that person to disclose or use a current or former employer's trade secrets improperly or violate any confidentiality or non-competition agreement. You are prohibited from improperly using anyone's trade secrets or violating any confidentiality or non-competition agreement in any work for the Company.

Reporting Breaches of Confidentiality and Security

You must immediately report any confidentiality, privacy, or security event under the Company's incident reporting procedures by sending an email to #incidentmanagement (GRP-IncidentManagement@ghx.com). Immediate reporting may help limit or prevent damage and compliance issues. In addition, the Company may have legal or business obligations to notify third parties or regulators of certain incidents within a very short period.

Disclosing Trade Secrets in Whistleblower and Retaliation Claims (U.S. Only)

Under the U.S. Defend Trade Secrets Act of 2016, U.S. Personnel will not be held criminally or civilly liable under any U.S. federal or state trade secret law for the disclosure of a trade secret that: (a) is made (i) in confidence to a U.S. federal, state, or local government official, either directly or indirectly, or to an attorney; and (ii) solely for the purpose of reporting or investigating a suspected violation of law; or (b) is made in a complaint or other document that is filed under seal in a lawsuit or other proceeding. U.S. Personnel are further notified that if you file a lawsuit for retaliation by an employer for reporting a suspected violation of law, you may disclose the employer's trade secrets to your attorney and use the trade secret information in the court proceeding if you: (a) file any document containing the trade secret under seal; and (b) do not disclose the trade secret, except pursuant to court order.

Social Media

Social media has become a key method for individuals and companies to communicate publicly. Keep in mind that your use of social media could impact both you and the Company, sometimes in unintended ways.

Do not disclose confidential and/or proprietary information about our business, our people, our suppliers, or our customers. Be clear about your role at the Company. Any time you mention the Company on social media, unless you are in a role designated to speak publicly on behalf of the Company, you must be clear you are not authorized to represent the Company, using language in your profile or posts such as “All views expressed here are my own and not those of my employer.” For additional information, please review the GHX North America Social Media Policy.

Records Management

You generate many records in your work for the Company, in the form of computer files, emails, direct messages, texts, voice mails, hard-copy documents, etc. Some laws and contracts require records to be maintained for a certain period, and some require records to be securely destroyed when no longer needed. Certain records and related storage media must be disposed of according to specific security standards. Balancing these requirements with business needs requires active records management. You should confer with the Compliance Department with any questions about records retention and disposal requirements, including about related Company policies and guidelines.

You should always think before you say or write anything that could be misinterpreted. Avoid exaggeration, derogatory remarks, guesswork, or inappropriate characterizations that can be misunderstood or misconstrued. A good rule of thumb is to imagine how you would feel if what you are doing or saying were to become widely known to your friends and family or to appear in the news.

From time to time, the Company’s Legal Department may issue legal holds that require preservation and production of certain Company records. If you receive notice of a legal hold, you must immediately comply with its terms, including avoiding any behavior that may possibly be construed as destroying or hiding potential evidence. Be aware that even opening or moving electronic files, including emails and documents, may alter their data and inadvertently create evidentiary issues. Contact the Company’s Legal Department with any questions or concerns regarding legal holds.



Employment and the Workplace Environment



Employment and the Workplace Environment

We all must collaborate to maintain a professional work environment in compliance with applicable law and ethical standards. Keep in mind that the workplace environment can extend beyond Company offices to customer sites, Company events, remote working sites, online and telephone conversations, and cyberspace.

The laws applicable to workplace conduct may vary by jurisdiction. The Company expects all employees to familiarize themselves and comply with any Company Employee Handbook applicable to their jurisdiction, as well as all applicable contracts and agreements governing their workplaces. You should refer to the applicable Employee Handbooks and/or employment contracts for further details.



Hiring and Contracting

To help the Company engage high-quality employees, only a small number of Company personnel have the authority to make an employment offer to anyone, and offers must be made in certain forms:

- in North America, only a Company officer or the Chief People Officer can make an employment offer, and the official offer must be in the form of a written offer letter.
- in Europe, every employment offer must be preapproved by the Manager, People Excellence HR in Europe and approved and signed by the GHX Europe President. Only the members of the European Human Resources Department can extend the offer. The offer must either be in writing or accompanied by a written agreement.
- in India, every employment offer must be approved and signed by the Director, India Human Resources. For positions Director level and above, in addition to the Director, India Human Resources, every employment offer must also be approved by India's VP, MD & IN Country Head and US, Director of Total Rewards. Only the members of India's Human Resources Department can extend the offer. The offer must either be in writing or accompanied by a written agreement.

Only the Company President (or his or her authorized designee) or, in Europe, the GHX Europe President (or his or her authorized designee), has the authority to execute an employment agreement, including any employment agreement for any specified period of time. Only an authorized signatory for the relevant GHX entity may sign any agreement to engage a vendor, including any consulting engagement.

Misclassifying individuals' employment status can lead to penalties and other liability. To avoid these problems, you must follow established Company policies and procedures on contractor engagement, including documentation requirements. If you have questions about personnel contracting, you need to confer with the Human Resources and Legal Departments.

Depending on applicable law and the facts and circumstances of each case, certain convictions, debarments, sanctions, or other penalties may make an individual or company ineligible to do business with the Company. In some jurisdictions, the need to avoid conflicts of interest, discrimination, and harassment may restrict engagement of relatives and certain workplace dating relationships. Please refer to the appropriate Employee Handbook and/or your local Human Resources Department for the rules applicable to you.

Selection and Use of Third Parties

The Company believes in doing business with third parties that demonstrate ethical business behavior and support our mission, vision, and values. You should keep these standards in mind when selecting vendors and other third parties for business opportunities and monitor their performance throughout the relationship. Vendor security review requests should be submitted for all new vendor engagements, as well as any significant changes to existing vendor engagements (e.g., addition to, or change of, GHX data hosting, new software or SaaS services, material change to other vendor-provided services). Our reputation and our customers depend on us enforcing our standards with these third parties. We offer fair opportunities for prospective third parties to compete for our business. The way in which we select our suppliers and the character of the suppliers we select reflect on the way we conduct business.

Non-Discrimination and Anti-Harassment

We are an equal opportunity employer. We strive to keep our workplace environment free from unlawful discrimination and harassment, in compliance with the laws that apply to each GHX entity. You are prohibited from engaging in illegal discrimination and harassment, including on the basis of any status protected by applicable country, state, provincial, or local law. Protected status may include age, race, color, national origin, gender, gender identity, sexual orientation, religion, mental or physical disability, pregnancy, or other characteristics. The Company will make reasonable accommodation for qualified individuals with known disabilities, unless doing so would result in an undue hardship for the Company or, in the U.S., would present a direct threat. You should refer to the applicable Employee Handbooks, employment contracts and/or discuss with the local Human Resources Department for further details about our non-discrimination and anti-harassment policies. See the "Reporting and Investigations" section of this Code of Conduct for a description of your obligations to report and to not retaliate against anyone making a good-faith report of misconduct.

Committed to Human Rights

We are committed to upholding fundamental human rights and believe that all human beings around the world should be treated with dignity, fairness, and respect. We ask that our vendors and contractor personnel demonstrate a commitment to the health and safety of their workers and operate in compliance with human rights laws. The Company does not use or condone the use of slave labor, child labor, human trafficking, human smuggling, or any form of modern slavery, and denounces

any degrading treatment of individuals or unsafe working condition. The Company's current Modern Slavery Act Transparency Statement is posted on the European section of our website.

We are committed to following all applicable wage and hour laws and regulations. Anyone paid based on hours worked must report and record all time worked accurately in accordance with established local procedure.

Physical Safety and Health

Maintaining a safe workplace also requires collaboration. Your part includes following applicable environmental, safety, and health laws and regulations, and observing the Company policies regarding identification badges, facilities access, and reporting accidents, injuries, and unsafe conditions. Personnel and visitors must observe applicable restrictions on weapons, smoking, and alcohol and drug use on Company property, including parking lots and vehicles. You should refer to the applicable Employee Handbooks and employment contracts and/or discuss with the local Human Resources Department for further details.

Unless applicable law requires otherwise, neither you nor visitors have a right to or expectation of privacy on Company property (including while in Company offices and parking lots) and while using Company IT resources. To the extent allowed by applicable law, the Company may monitor, search, and manage use of Company resources and any data created, stored on, or accessed using them. See "GHX Resources — In General" [on page 18](#).

In North America, to the extent allowed by applicable law, the Company:

- maintains video surveillance on some Company property;
- reserves the right at any time and at its discretion to search all Company-owned or leased property and any people, vehicles, and other property entering on or accessed using Company property or in conducting Company business, with entry onto Company property constituting consent to searches and questioning; and
- may discipline Personnel if they refuse to cooperate with or consent to search or attempt to destroy potential evidence (other than in accordance with applicable law, Company policies and procedures, and any legal holds in effect).

You should immediately report to the Company (and to law enforcement, where appropriate) any potential threat to safety or health on Company property or affecting Company business. See "Reporting and Investigations" [on page 29](#). Refer to the applicable Employee Handbooks and employment contracts and/or discuss with your HR Business Partner for further details.

Reporting and Investigations



Effective Lines of Communication & Reporting

Duty to Report

Maintaining our culture of compliance requires you to take an active role in trying to prevent and promptly address any violations. If you are seeking guidance, have a concern, know of or suspect any violation of applicable law or policy (including this Code of Conduct), report it to the Company right away. We provide numerous reporting options so you can report concerns in whatever way makes you the most comfortable.

Managers at the Company must carry out the following actions when an employee raises a concern or brings something to your attention to assure them they have made the right decision in approaching you:



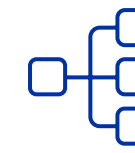
Listen Carefully: Thank the person for taking the difficult decision of speaking up, even if you disagree with them. Listen closely to what they have to say and show that you're focused on resolving the issue.



Maintain Confidentiality: To the extent possible, protect the colleague's privacy. Avoid discussing the conversation with others on your team.



Be Objective: Continue to treat all employees with the same degree of fairness, including if they've reported a concern or are the subject of a report.



Escalate to the Right Channels: While you may be tempted to take ownership of the concern, you must assess whether it needs to be escalated to HR or a designated department from the chart [on page 31](#). If you have questions or are not sure if you can resolve a concern on your own, consult your HR Business Partner, Compliance, or the Legal Department.

The following departments are designated to receive reports of violations of applicable law or this Code of Conduct in the areas listed. Your local HR Business Partner can provide contact details if you need them. Please immediately report any potential security or privacy incident by emailing [#incidentmanagement \(GRP-IncidentManagement@ghx.com\)](#).

Where to Report¹

	GHX Department					
	Human Resources	Legal Department	Chief Financial Officer or Controller	Compliance Department	Enterprise Technology	#incidentmanagement (GRP-IncidentManagement@ghx.com)
Areas of Responsibility	<ul style="list-style-type: none"> • Workplace environment • Discrimination • Harassment 	<ul style="list-style-type: none"> • Antitrust • Government investigations / subpoenas / legal notices • Crimes • Insider trading • Import/export • Misconduct by any senior management team member 	<ul style="list-style-type: none"> • Financial issues 	<ul style="list-style-type: none"> • Anti-corruption • Confidentiality / privacy issues • Conflicts of interest • Complaints from customers, vendors, or other third parties • Fraud / bribery / kickbacks 	<ul style="list-style-type: none"> • Technology issues 	<ul style="list-style-type: none"> • Security or privacy incidents

¹Employees should also refer to their applicable regional Employee Handbook for additional guidance on appropriate reporting processes and procedures.

If you're not sure where to report, or if the designated official may have a conflict of interest on the matter, you may first report to your manager; the Compliance Department; the Legal Department, the Human Resources Department; or through the Compliance and Ethics Hotline at <https://secure.ethicspoint.com/domain/media/en/gui/22459/index.html> or by toll-free telephone at:

United States, Canada (English), Guam, and Puerto Rico	888-278-3164
Canada (French)	855-350-9393
Belgium	0800-77004
Germany	0800-1016582
Netherlands	0800-0226174
Switzerland	0800-562907
United Kingdom	0800-032-8483

The Compliance and Ethics Hotline will provide the information to the Company on a confidential and anonymous basis to the extent allowed by applicable law. Please note that the laws of some countries restrict anonymous reporting of certain issues. Company policy is to comply with applicable law governing reporting, including applicable data privacy law.

Non-Retaliation

You are prohibited from retaliating against anyone who has made a good-faith report of misconduct or assisted in an investigation. The Company will impose appropriate disciplinary measures against any Personnel who knowingly and with intent to retaliate take any harmful action against another person for providing good faith information relating to potential violations of Company policy or applicable law. Such measures may include termination of employment, referral to appropriate governmental authorities, and civil action for damages and other remedies, subject to applicable law.



Investigations & Response

Investigations

Please include enough detail in your report (e.g., names, dates, places) to allow a good investigation. The Company will determine whether an investigation is appropriate and its scope. No Personnel should attempt to conduct their own investigation and should not access any electronic data that may relate to the allegation. No Personnel who may be involved in or have a conflict of interest connected with a reported potential violation may be involved in investigating it.

The Company will try to keep investigations confidential to the extent it does not impede an efficient process and is allowed by law. It may not always be possible to keep an investigation confidential. An investigation can include speaking with the reporting individual, conducting witness interviews, interviewing the accused, reviewing relevant documentation, and consulting with subject matter experts. If you have concerns about whether or how a report you have made is being dealt with, please contact Human Resources, Compliance, or the Legal Department.

We ask all Personnel to cooperate fully with any Company internal investigation or audit. This means providing truthful and complete information that may be relevant, participating in requested interviews, and preserving all potentially relevant records and data. You may not improperly influence any Company investigation or audit. All investigations should be done in a timely manner without unreasonable delays and in accordance with regulatory requirements.

All search warrants, subpoenas, court orders, inquiries by government officials, and other forms of legal process must be brought immediately to the Legal Department. If you learn of any external investigation or audit, you should immediately inform the Legal Department before speaking with any outside person about it, unless prohibited by law. Government investigators sometimes approach individuals outside of work. If government representatives contact you about the Company, we would appreciate it if you would notify the Legal Department before you speak with the government and would also appreciate having Company legal counsel included in any such discussions, to the extent permitted by law. You may also wish to retain your own legal counsel before such discussions.

Enforcement & Disciplinary Action

Disciplinary Action

If the Company determines that a violation of applicable law or policy has occurred, the Company will decide at its sole discretion what disciplinary action to impose, subject to applicable law. Disciplinary action may range from a verbal reprimand up to and including termination of employment or contract. The Company also reserves the right to report to the appropriate governmental authorities and seek civil damages or other relief.

Corrective Action

GHX has the right to take appropriate actions to respond to any noncompliance identified, which may include further investigation through legal counsel, disciplinary action, revisions to policies or practices, trainings, reporting and returning overpayments, and/or the involvement of appropriate government agencies. If the investigation uncovers violations of applicable laws, rules or regulations, the Compliance Officer shall report the conclusions to the Compliance Committee and Board of Directors. Legal counsel may be contacted to determine whether disclosure or repayment to the appropriate government entity should be made.



Change Control Grid

Version Date	Summary of Revisions	Approved By (Name, Title)
5/29/12	Original Issuance	Board of Directors
7/29/13	Eliminated duplicative provisions now included in new or revised policies and procedures	Chris McManus, Vice President, General Counsel
3/25/15	Reviewed and updated	Chris McManus, Vice President, General Counsel
9/30/16	Reviewed and updated including applicable Company Personnel and locations worldwide	Chris McManus, Vice President, General Counsel
1/25/17	Minor content changes requested by GHX Europe	Chris McManus, Vice President, General Counsel
4/27/18	GDPR-specific language added	Chris McManus, Vice President, General Counsel
9/11/20	Simplified and updated language and added examples	Chris McManus, Vice President, General Counsel
7/13/22	Reviewed and updated	Chris McManus, Vice President, General Counsel
8/29/23	Updated letter from the CEO and money laundering and terrorism financing language added	Heather French, General Counsel and Corporate Secretary
9/19/24	Reviewed and updated content to meet industry standards.	Heather French, Chief Legal Officer and Corporate Secretary