

# Innovative

Management Systems



## Code of Conduct

Created: 09/27/2019

Revised: 04/10/2020, 09/15/2020, 05/21/2021, 10/01/2021, 10/08/2022

## Table of Contents

|  |    |
|--|----|
| <b>I. Message from the Managing Principal</b> .....                                  | 4  |
| <b>II. About the Code of Conduct</b> .....   | 5  |
| <b>III. Doing the Right Thing</b> .....  | 5  |
| <b>1. Values that Guide Us</b> .....   | 6  |
| <b>IV. HIPAA Confidentiality, Privacy, and Security</b> .....                        | 6  |
| <b>1. Definitions</b> .....  | 7  |
| <b>2. Privacy Rule</b> .....   | 7  |
| <b>3. Security Rule</b> .....  | 8  |
| <b>4. Breach Notification Rule</b> .....   | 8  |
| <b>5. Ways You can Minimize the Risk of Potential HIPAA Breaches</b> .....           | 8  |
| <b>6. Failing to Adhere to Policies</b> .....  | 9  |
| <b>7. Storing Confidential Information Correctly</b> .....                           | 9  |
| <b>V. Focused Response on Member and Member Care</b> .....                           | 10 |
| <b>1. Detect and Prevent Fraud, Waste, and Abuse</b> .....                           | 10 |
| <b>2. Follow Anti-Fraud Laws</b> .....   | 10 |
| <b>3. Reporting Fraud, Waste and Abuse</b> .....                                     | 10 |
| <b>4. Investigation</b> .....  | 10 |
| <b>5. Disclosures when Serving in the Board of Directors of Another Entity</b> ..... | 11 |
| <b>VI. Protecting Assets and Information</b> .....                                   | 11 |
| <b>1. Safeguarding and Using IMS' Assets and Information</b> .....                   | 11 |
| <b>2. Use Information Systems Appropriately</b> .....                                | 11 |
| <b>3. Safeguarding Confidential Information</b> .....                                | 12 |
| <b>4. Keeping Track of Assets</b> .....  | 12 |
| <b>5. Using Funds Appropriately</b> .....  | 12 |
| <b>6. IMS Facilities</b> .....   | 12 |
| <b>7. Maintaining Accurate Business Records</b> .....                                | 12 |
| <b>8. Records Retention and Destruction According to Policy</b> .....                | 13 |
| <b>VII. Protect IMS' Reputation</b> .....  | 13 |
| <b>VIII. Respect for One Another</b> .....   | 13 |
| <b>1. Workplace Diversity</b> .....  | 13 |
| <b>2. Harassment is Prohibited</b> .....   | 13 |
| <b>3. Retaliation – What about it?</b> .....   | 14 |

|   |    |
|---|----|
| <b>IX. Cultural Competence</b> .....                              | 14 |
| <b>1. Definitions</b> .....                                       | 14 |
| <b>2. Identify</b> .....  | 15 |
| <b>3. Expectations</b> .....                                      | 15 |
| <b>X. Conflict of Interest</b> .....                              | 17 |
| <b>1. Gifts and Business Courtesies</b> .....                     | 17 |
| <b>2. Members Gifting Employees</b> .....                         | 18 |
| <b>3. Employees Gifting Others</b> .....                          | 18 |
| <b>4. The Workplace and Personal Relationships</b> .....          | 18 |
| <b>5. Relatives Who Work for Vendors</b> .....                    | 18 |
| <b>6. Other Employment</b> .....                                  | 19 |
| <b>7. Follow Anti-Kickback Laws</b> .....                         | 19 |
| <b>XI. Government Inquiries and Meeting Expectations</b> .....    | 19 |
| <b>1. Interacting with Government Officials</b> .....             | 19 |
| <b>2. No Gifts for Government Officials</b> .....                 | 21 |
| <b>3. Accurate and Timely Reporting to the Government</b> .....   | 21 |
| <b>XII. Follow Licensing and Certification Requirements</b> ..... | 21 |
| <b>1. Convicted of a Crime</b> .....                              | 21 |
| <b>XIII. Healthcare Sanctions/Exclusion Checks</b> .....          | 21 |
| <b>XIV. Reporting Suspected Compliance Issues</b> .....           | 22 |
| <b>1. IMS' Compliance Hotline: (1-855-222-1025)</b> .....         | 22 |
| <b>XV. Summary of the Code of Conduct</b> .....                   | 23 |
| <b>XVI. IMS Employee Resources</b> .....                          | 23 |

## I. Message from the Managing Principal



We are fortunate to be given the opportunity to provide the health care services to address the needs of the vulnerable individuals of our community through our organization, Innovative Management Systems. I urge and invite you to read and understand our Code of Conduct (“Code”). The Code will be our guiding principle as we perform our daily tasks and functions.

Acting with integrity, performing ethically, and meeting compliance requirements in all we do will help protect our members, our resources, and our name in the communities we serve.

Thank you for the work and care you provide every day.

Sincerely,

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

**Lee Suyenaga, Managing Principal**

## II. About the Code of Conduct

Innovative Management Systems' Code of Conduct provides guidance about the business conduct expected of employees and the workforce during work and in the course of interactions with others. This Code of Conduct works alongside other Company resources, including:

- IMS Departmental Policies and Procedures:
  - X:\!IMS Policy and Procedures [ALL EMPLOYEES]
  - Y:\!IMS Policy and Procedures [ALL EMPLOYEES]
  - S:\!IMS Policy and Procedures [ALL EMPLOYEES]
- IMS Employee Handbook.

The Code of Conduct is reviewed and approved by the Compliance Delegation Oversight Committee (“Committee” or “CDOC”) and Executive Management and is updated as needed to incorporate changes to applicable laws and regulations. Employees will be notified of any updates to the Code of Conduct.

## III. Doing the Right Thing

The successful business operations and reputation of **Innovative Management Systems** (“IMS”) is built upon principles of fair dealings and the ethical conduct of our employees. We are strongly committed to “doing the right thing” and we will do our best to conduct ourselves with the highest standards of conduct and personal integrity. We also strive for excellence, which requires careful observance of the spirit and letter of applicable laws and regulations.

This Code of Conduct will be used as a tool to ensure that compliance is integrated into our day-to-day work – whether it is care, service, or any operational duties such as communications or business processes. This applies to all IMS workforce, regardless of whether one is the executive of a department, a salesperson in marketing, an officer, a director, or a staff assistant. All workforce members should refer to this Code of Conduct when conducting daily business operations and dealings.

Employees who experience situations that are not included in this Code of Conduct must contact any of the following for additional guidance:

- Your immediate supervisor/director
- Human Resources Department
- Management team
- Compliance Department
- Call or submit a report (may be anonymous) via the Compliance Hotline at (844) 359-3410.  
This number is toll-free and available 24 hours a day, 7 days a week.

Everyone is accountable for compliance and no one is exempt. All workforce members who work for or on behalf of IMS are required to adhere to all applicable laws, policies and procedures, and this Code of Conduct. This includes permanent employees, temporary employees, contingent employees, and interns, if any.

All employees are accountable for their actions and must conduct business with the highest integrity and with the members' best interest in mind. Employees must also:

- Complete all required compliance training.
- Familiarize themselves with the policies, procedures, and standards that apply to their work.
- Address any concerns, if unsure about what they are being asked to do or what they see others doing.
- Cooperate with investigations of alleged or potential violations of law or Company policy.
- Not participate in illegal or unethical acts.
- Protect IMS' reputation and assets.

Failure to adhere to or comply with this Code of Conduct could result in disciplinary action, up to and including termination of employment. These consequences may also apply to any employee who tries to retaliate against someone who has reported potential violations in good faith.

## 1. Values that Guide Us

- a) Our Members' Health – We work to provide our members with the best service, and to improve access and delivery of health care.
- b) Continuous Learning – Our commitment and dedication to continuous improvement and learning/training will raise our standards of our profession. We give our best efforts to improve our skills and knowledge to serve our members, our organization, our business partners, and each other.
- c) Teamwork – Collaborating with others is where we can be most effective. Together, we can go further and achieve our goals.
- d) Respect our Members, Business Partners, and One Another – We do our best to be courteous and act with the utmost professionalism and consideration in our manners.
- e) We grow and succeed professionally, and personally, when we respect one another.
- f) We all have varying points of view, but we must respect and listen to these varying opinions.
- g) Be fair and honest – We must earn our reputation every day and understand that each health care and business decision is an opportunity to demonstrate our commitment to ethics and integrity. We recognize the trust others place in us and recognize the responsibility of upholding that trust by being truthful and honest – always.
- h) Commitment to Compliance and Ethics: Compliance means to fully adhere to federal, state, and local laws and regulations; federal health care program requirements; licensing requirements; accreditation standards; the requirements of the Centers for Medicare and Medicaid Services (“CMS”), and federal, state, and business partners' contracts.
- i) Retaliation against those, who in good faith, report suspected violations of this Code of Conduct, laws and regulations, accreditation standards, and/or IMS policies is prohibited.
- ii) We act with ethics and integrity in our work. We always try to do the right thing and make the best decisions. We seek help by referring to this Code of Conduct or the advice of other personnel or Management when the right thing or the best decision is not clear.

## IV. HIPAA Confidentiality, Privacy, and Security

Our members' protected health information (“PHI”) is very sensitive and protected under privacy and information security laws. Additionally, we must abide by any business associate agreements that we have with other business entities as part of doing business. Keeping data confidential, private, and secure is very important to ensure that we:

- Preserve the trust of our members.
- Provide quality health care.
- Comply with federal and state regulations and IMS' policies.

All employees will undergo training regarding handling PHI, including electronic PHI (ePHI), through departmental training and/or new hire orientation. It is everyone's responsibility to ensure that PHI and ePHI are not used in a manner that is not in accordance with the IMS' Code of Conduct and the law.

## 1. Definitions

- **Availability:** ePHI is accessible and usable on demand by authorized persons.
- **Breach:** an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of PHI.
- **Business Associate:** a person or organization, other than a workforce member of a covered entity, that performs certain functions on behalf of, or provides certain services to, a covered entity that involve access to PHI. Can also be a subcontractor responsible for creating, receiving, maintaining, or transmitting PHI on behalf of another business associate.
- **Confidentiality:** ePHI is not available or disclosed to unauthorized persons or processes.
- **Covered Entity:** must follow HIPAA rules. Includes covered health care providers, health plans, and health care clearinghouses.
- **HIPAA:** also known as the "Health Insurance Portability and Accountability Act," includes Privacy, Security and Breach Notification Rules that protect the privacy and security of health information and provide individuals with certain rights to their health information.
- **Integrity:** ePHI is not altered or destroyed in an unauthorized manner.
- **PHI/ePHI** – protected health information/electronic protected health information; no matter the type of PHI (electronic, paper, or verbal), PHI encompasses all of the following:
  - Individual's past, present, or future physical/mental health or condition
  - Provision of health care to the individual
  - Past, present, or future payment for the provision of health care to the individual
  - Common identifiers, such as name, address, birth date, and Social Security number

## 2. Privacy Rule

All employees and/or affiliates of IMS must respect the PHI of those affiliated with us. Individuals have important rights with respect to their PHI, including the right to examine and obtain a copy of their health records in the form and manner they request, and to ask for corrections to their information.

The HIPAA Privacy Rule establishes standards to protect PHI held by covered entities and their business associates. The Privacy Rule also permits the use and disclosure of health information needed for patient care and other important purposes. This includes the "minimum necessary" standard which requires that when a covered entity or business associate uses or discloses PHI, or when it requests PHI from another covered entity or business associate, the covered entity or business associate must make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

Before making any updates or changes to member information, it is important to ensure that the individual is a member within IMS' network, as we only assist those that are in our network. Employees

must also ensure that any documents or data containing PHI are sent to us in a secured manner. When sending any emails containing any member PHI to external parties, please ensure that you include “[SECURE]” in the subject line of your email. This will ensure that the email is encrypted and sent in a secure manner. If you have any questions, it is important to check with your immediate supervisor/director for any further directions or clarification before using, disclosing, and handling PHI/ePHI.

### 3. Security Rule

The HIPAA Security Rule specifies safeguards that covered entities and business associates must implement to protect ePHI confidentiality, integrity, and availability. There must be reasonable and appropriate security measures, through policies and procedures, to protect the security of EPHI that is created, received, maintained, or transmitted.

IMS will always authenticate specific information to prove that covered entities, including business associates, are contracted/affiliated with us through appropriate security measures, and through policies and procedures created.

It is also important that the access/transfer of any PHI/ePHI is under protected secured network. Only employees that have been approved by the Managing Principal may utilize other means of accessing/transferring sensitive information, and they will need to follow procedures in place, such as installing approved security programs, before being able to work with PHI/ePHI.

### 4. Breach Notification Rule

The HIPAA Breach Notification Rule requires covered entities to notify affected individuals, the U.S. Department of Health and Human Services (“HHS”), and in some cases, the media, in the event that there is a breach of unsecured PHI. A breach is an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of PHI. The impermissible use or disclosure of PHI is *presumed* to be a breach unless you demonstrate that there is a low probability that the PHI has been compromised based on a risk assessment.

Employees and/or affiliates must notify the IMS Compliance Department in the case of a potential or actual HIPAA breach so that IMS may take appropriate measures to investigate and mitigate the issue, and to provide notification to the appropriate parties.

If you think there has been a potential or actual HIPAA breach, you must report the issue immediately to your immediate supervisor/director **and** the Compliance Department. You can also call the Compliance Hotline at 844-359-3410 to file a report. Upon notification of a potential breach, the IMS Compliance Department will conduct an investigation, and will determine whether it is a reportable breach by completing a HIPAA risk assessment.

### 5. Ways You can Minimize the Risk of Potential HIPAA Breaches

Listed below are some examples of measures that employees can take to minimize the risk of potential HIPAA breaches:

- Access and use the minimum amount of PHI necessary to do your job, whether performing administrative and/or business duties.



- Use confidential information or protected health information (PHI) only with proper security authorization.
- Ensure any emails containing PHI are sent securely to external parties by including “[SECURE]” in the subject line of the email.
- Discuss member information:
  - Only when it is required by the job.
  - Only when federal and state laws permit you to do so.
- Keep electronic devices password protected and secure.
- Make sure doors to restricted areas where sensitive information is kept are locked.
- Retrieve printouts containing PHI promptly from shared fax machines and printers, and never leave any printouts behind.
- Discard any documents containing PHI in the designated shredding bins.
- Use a privacy screen on employees’ computer monitors if the screen is visible and readable by others.
- Log off a shared computer or lock your computer before walking away from it so others cannot use it.
- Restrict access by vendors (if applicable) to PHI unless an appropriate process has been followed (for example, completing a business associate agreement (BAA)).

If you have further questions or concerns regarding PHI and HIPAA, please ask your immediate supervisor/director, Human Resources Department, and the Compliance Department.

## 6. Failing to Adhere to Policies

Employees are expected to abide by the requirements of HIPAA, other applicable privacy and security laws, and IMS’ policies on confidentiality, privacy, and security. Failing to adhere to these policies may result in:

- Disciplinary Action
- Termination of Employment
- Criminal prosecution by the Office of Civil Rights, state attorney general, or United States attorneys.
- Prison time
- Sanctions

## 7. Storing Confidential Information Correctly

Confidential information, such as PHI, should be stored on IMS’ secured network and servers only. IMS discourages the use of storing confidential information on any other devices without the prior approval from the Managing Principal.

Once approval is received, the data on approved devices with appropriate security measures must be encrypted and must have other special physical and security steps in place, such as password-protection. This will protect any confidential and sensitive information from being accessed/misused if the device is lost or stolen.

## V. Focused Response on Member and Member Care

### 1. Detect and Prevent Fraud, Waste, and Abuse

IMS' Compliance Program protects our members from fraud and preserves IMS' resources from waste to reduce costs and help provide affordable health care. This part of our mission requires the involvement, commitment, and participation of every member of the IMS workforce. There is additional training provided to all employees on how to detect and prevent fraud, waste, and abuse.

### 2. Follow Anti-Fraud Laws

IMS workforce members must never participate in fraudulent activity at work. Employees must preserve IMS resources to provide the most affordable health care for our members. If you become aware of any fraudulent activity, it must be reported to your immediate supervisor/director **and** the Compliance Department immediately. You can also submit an anonymous report via the Compliance Hotline at **1-844-359-3410**. This is a toll-free number that is available 24 hours a day, 7 days a week.

The government's definition of fraud in a health care setting includes certain acts that are not intentional. For example, if IMS submits inaccurate data to the Centers for Medicare and Medicaid Services ("CMS") and receives reimbursement, it could be considered fraud, even if the submission of inaccurate data was accidental.

### 3. Reporting Fraud, Waste and Abuse

It is crucial to report any potential or actual fraud, waste, and abuse ("FWA") incident that is experienced and/or observed. There are multiple ways in which you may report potential or actual FWA incidents:

- **Email:** [Compliance@imsmsso.com](mailto:Compliance@imsmsso.com)
- **Phone Hotline:** 1-855-222-1025
  - This hotline is available 24 hours a day, 7 days a week
  - Reports can be made confidentially and **anonymously**
- **Online Reporting:** [www.lighthouse-services.com/imsmsso](http://www.lighthouse-services.com/imsmsso)
  - You can file a report on the web portal **anonymously**
- **Fax:** 1-323-832-8141
- **In-Person:** Reports may be made in person to the IMS Compliance Officer

IMS has a non-retaliation policy that states that there will be NO retaliation against you for reporting suspected non-compliance or FWA in good faith. Only those employees, who intentionally make false allegations/accusations with the purpose of harassing, discriminating, and/or retaliating against another individual, will be subjected to disciplinary actions, up to immediate termination. All reports made will be treated with the utmost discretion and confidentiality.

### 4. Investigation

Depending on the type of incident that was reported, it is the responsibility of the Directors, Human Resources Department, and/or Compliance Department to respond to and investigate reports within an appropriate amount of time. Investigations shall be handled by persons having sufficient level of

expertise/knowledge with regard to the issue presented. Appropriate action will be taken in response to the allegations and a corrective action plan will be created to resolve any/all issues, if necessary.

If applicable, the individual that reported the incident will be notified through a confidential manner. Depending on the nature and severity of the issue, IMS may notify appropriate outside agencies, law enforcement, or regulatory boards, and if necessary, any business affiliates, contractors, and/or health plans.

IMS will maintain documentation regarding these incidences for a minimum of ten (10) years after the investigation has been completed and closed.

## 5. Disclosures when Serving in the Board of Directors of Another Entity

If and when IMS workforce members, including the IMS' Board of Directors, want to voluntarily serve as a member of another entity's board of directors or an advisory board, it must be made clear that involvement with these entities is as an individual and does not necessarily represent the interests, values, or perspectives of IMS. Such workforce members must disclose, in writing, their involvement with such entities or organizations to their supervisor/director, Human Resources, and the Compliance Department, **if:**

- These activities conflict with the work or mission of IMS or with the employees' individual job responsibilities/functions.
- The position relates to an official city, county, state, or federal commission, board, or committee.
- The entity(ies) or organization(s) requests contributions in cash, goods, or services from IMS.

# VI. Protecting Assets and Information

## 1. Safeguarding and Using IMS' Assets and Information

IMS' assets are to be used for IMS' business purposes only. They must be handled with care and protected against all forms of loss, damage, waste, and misuse. Do not use IMS' assets for personal gain or benefit or dispose of assets outside of authorized practices regardless of condition or value. If IMS employees are aware of any fraudulent activity, it must be reported to your immediate supervisor/director **and** the Compliance Department.

## 2. Use Information Systems Appropriately

IMS' information systems include e-mail, voicemail, intranet, and access to Internet over the IMS network. These assets are tools for employees to use in providing health care to members and to conduct IMS business. All communications, including electronic communications on hand-held devices, must be conducted in a professional, respectful, and lawful manner that is appropriate in a business environment.

IMS' information systems should never be used to engage in activities that are illegal or illicit, that violate IMS' policies, or that could damage IMS' reputation or result in liability for IMS. It is prohibited to use IMS' e-mail, intranet, or the internet on IMS' computers for the following activities:

- Downloading music and videos for personal use.
- Accessing Twitter, Facebook, Instagram, and other social media/networking sites or applications for personal purposes.

- Downloading and/or running external software not approved by IMS' Information Technology Department.
- Viewing pornography or any other offensive, discriminatory, derogatory, or exploitative content.
- Bidding or purchasing items other than for IMS business use (i.e. eBay, Craigslist, and so forth).
- Gambling
- Sending mass e-mails asking co-workers to support personal or professional causes.

When using IMS' information systems, all data communications – including e-mail and voicemail messages – become the property of IMS and can be monitored and reviewed. Please see the IMS Employee Handbook for more information.

### 3. Safeguarding Confidential Information

Confidential information, such as IMS' financial data and reports, strategies, initiatives, and similar material, should not be shared with anyone outside the organization unless you have obtained written approval to disclose from the Managing Principal. When in doubt, please confirm with your immediate supervisor/director, Human Resources, and/or the Compliance Department.

### 4. Keeping Track of Assets

All IMS employees, from the workforce to the management teams, have a responsibility to keep track of the assets issued to them and/or to their department/personnel. They are also responsible for ensuring that the Company's property is not damaged. All of IMS' assets must be returned upon leaving IMS.

### 5. Using Funds Appropriately

Funds and other financial assets under IMS must be protected and handled responsibly, honestly, and in strict compliance with IMS' policies, including this Code of Conduct.

### 6. IMS Facilities

The safety of our employees/workforce, members, and assets must be protected. There are physical safeguards in place in order to do this:

- Facility access to the IMS suite is locked. Only IMS employees and their approved guests will be able to gain access into the suite by utilizing a RFID keycard access issued to them.
- You must always wear your work or identification badge. If you have lost your work or identification badge, you must report it immediately to your immediate supervisor/director and/or Human Resources.
- Do not provide unauthorized individuals with access to IMS facilities. Only approved guests of IMS will be able to access the facility. Employees will be notified when guests are to be expected.
- If employees become aware of unauthorized access to IMS' facilities, report this immediately to your supervisor/director, Human Resources, and/or the management team.

### 7. Maintaining Accurate Business Records

It is important to maintain accurate business records, filing timesheets, financial and statistical reports and information. IMS workforce members who provide data or information that is false or inaccurate are subject to discipline, up to and including termination of employment.

## 8. Records Retention and Destruction According to Policy

IMS records must be retained and destroyed according to federal, state, and local laws and regulations; applicable licensing, accreditation, and contractual requirements; and, applicable IMS policies. Never destroy, change, or conceal any record if you have been instructed to keep it, or if you know or think it is possible that the record may be involved in an investigation or litigation.

## VII. Protect IMS' Reputation

The public is protected from dishonest and deceptive marketing by federal, state, and local laws. IMS should ensure that it advertises its products and services in a consistent, strategic, creative, truthful, and accurate manner. Only authorized individuals/employees may communicate, directly or indirectly, to the public on behalf of IMS. Communication may include print advertising, publications, flyers, radio, television, and all other forms of communication not mentioned here. External communications must be reviewed and approved by the appropriate management or personnel. Some materials may also need to be reviewed by IMS' internal/external counsel, to ensure they have been approved by applicable federal and state agencies.

## VIII. Respect for One Another

All employees have a right to receive fair and just treatment and all employees have the responsibility to treat one another respectfully. This respect extends to our members and business partners, the community, and anyone who meets IMS.

### 1. Workplace Diversity

Employees' varying backgrounds and diverse ideas create a work environment where everyone grows. We make use of each other's talents, experience, and backgrounds to their full potential.

If employees believe that they have been subject to discriminatory conduct and/or witness such activity, report it immediately to your immediate supervisor/director, the Human Resources Department, and/or the Compliance Department. Supervisors and directors must immediately report allegations of discrimination to Human Resources regardless of who is engaged in the alleged misconduct.

### 2. Harassment is Prohibited

IMS does not tolerate harassment of any kind, as stated in IMS' policies and procedures. Whether an offense was intended or not, harassment – or the perception that it exists or has occurred – is harmful and creates a less effective work environment. More information can be found in IMS' Employee Handbook and Human Resources Policy & Procedure 70.09.01 – “Prohibiting Harassment, Discrimination, and Retaliation.”

Harassment takes many forms. Examples include:

- Verbal, physical, or visual conduct that disrupts another's work performance or creates an intimidating, harassing, or hostile environment.
- Communicating or displaying offensive material in the workplace.
- Unwelcome sexual advances, sexual remarks, displays of offensive material requests for sexual favors, and other unwelcome verbal or physical conduct of a sexual nature.
- Jokes, insults, threats, and inappropriate comments about a person's race, color, sex, gender identity, age, religion, national origin, ancestry, citizenship, physical or mental disability, veteran

status, sexual orientation, genetic information, or other status protected by applicable federal, state, or local laws.

If any employee is a victim of workplace harassment, or sees or hears it taking place, report it immediately to your supervisor/director, Human Resources, and/or file a report through the Compliance Hotline anonymously at 1-844-359-3410.

### 3. Retaliation – What about it?

IMS prohibits retaliation of any kind against individuals or employees who in good faith report or participate in the investigation of any complaint. This includes retaliation between peers, immediate supervisors/directors and employees, business partners and employees, and so forth.

If an employee believes that he or she, or others, are being retaliated against in any way for reporting or participating in the investigation of suspected illegal, unethical, or otherwise inappropriate acts, report it immediately to your supervisor/director or Compliance Department, or call the Compliance Hotline at 1-844-359-3410.

IMS is committed to creating a workplace where employees are protected from retaliation when they speak up against inappropriate or suspicious activities or when employees refuse to participate in wrongdoing. IMS employees are covered by the whistleblower protections under the Federal False Claims Act and other federal and state whistleblower laws and regulations.

The Federal False Claims Act is intended to reduce fraud, waste, and abuse of federal funds by allowing private parties to sue on behalf of the government against people or businesses alleged to have committed fraud. The act also protects whistleblowers from retaliation by employers for reporting potential violations or non-compliance in good faith.

## IX. Cultural Competence

IMS participates in the State's efforts to promote the delivery of services in a culturally competent manner to all members, including those with limited English proficiency, diverse cultural and ethnic backgrounds, disabilities, and regardless of gender, sexual orientation or gender identity. IMS' employees and those that are affiliated with us are to treat everyone courteously, with respect, and understanding, no matter the circumstances. We are providing services and care to members and our affiliates with diverse values, beliefs and behaviors, which means that our Company should also meet the members' and our affiliates' social, cultural, and linguistic needs. By doing this, can we reduce racial and ethnic disparities and present a good business culture. Employees are required to review and agree to this Cultural Competence policy, upon hire and on an annual basis thereafter.

### 1. Definitions

- **Culture** is defined as an integrated pattern of human behavior that includes thoughts, communications, languages, practices, beliefs, values, customs, courtesies, rituals, manners of interacting, roles, relationships and expected behaviors of a racial, ethnic, religious, social or political group
  - Some factors include but are not limited to age, gender, socioeconomic status, ethnicity, national origin, religion, geographical location, migration, sexual orientation, gender identity.

- **Cultural Competence** is defined as the ability of health care providers and health care organizations to understand and respond effectively to the cultural and linguistic needs brought by members through health care encounters. It is the ability to interact with people across cultures, with diverse values, beliefs, and behaviors.
- **Disability** is defined as a person that has a physical, developmental, mental impairment, diagnosed disability, temporary disability, a handicap that substantially limits one or more major life activities, has a record of such impairment, or is regarded by others as having such an impairment.
- **Effective Communication** is defined as the successful joint establishment of meaning wherein members, employees, and/or healthcare providers/affiliates exchange information, enabling members to participate actively in their care of service and ensuring that the responsibilities of members, employees, and/or healthcare providers/affiliates are understood.
- **Ethnicity** is a group having a common cultural heritage or nationality, as distinguished by customs, language, common history, etc.
- **Interpretation** is defined as the conversation of a message spoken in a source language into an equivalent message in the target language.
- **Race** is defined as any of the different varieties or populations of human beings distinguished by physical traits such as hair color and texture, eye color, skin color, or body shape.
- **Translation** is defined as the conversion of written text from one language into another.

## 2. Identify

In order to provide services in a culturally competent manner, it is important for IMS to identify the following:

- Race and/or ethnicity;
- The preferred language and method for oral and/or written communication, if not English;
- If there is the presence of any significant vision, hearing/speech, or cognitive impairment;
- If a proper language interpreter is needed for interpreter services; **AND/OR**
- Inquiring if there are any other accommodations needed that IMS should be aware of.

IMS takes a proactive stance in identifying some cultural competencies by doing the following:

- Presenting individuals who call IMS with multiple languages to choose from for interpretation needs.
- Having internal interpreters/translators that have been tested/certified to assist with interpreter services.
- Allowing service animals within the Company's premises.
- Having external professional translator/interpreter services available if internal interpreters/translators are unavailable.

## 3. Expectations

- **Communication Services**

IMS recognizes the importance of ensuring accessibility to individualized, high quality services for all members and their families. We are committed to providing special communication services to members with language and/or communication barriers. It is IMS' expectation to ensure that

effective communication is provided between the Company, its affiliates, and/or member(s) in a culturally competent manner through the following methods:

- For those with Limited English Proficiency (LEP), IMS can provide over-the-phone interpreter services through internal translators/interpreter services and/or professional third-party translator/interpreter services if the requested language is unavailable via an internal translator/interpreter.
- Any marketing materials that are sent out to members from IMS, and/or joint materials between healthcare provider(s), IMS, and/or the Health Plan(s), will be translated into the appropriate, preferred language.
- For those that are hard-of-hearing and/or deaf, IMS provides online services where members and/or family member(s) may reach us.
  - Requests for onsite American Sign Language interpreter services will require an advance notice of 5-7 business days.
- If these accommodations are still insufficient, IMS will work in good faith to accommodate any other disabilities and/or accommodations needed for members to receive effective communication that is culturally competent. IMS prefers advance notice of 5-7 business days so that we may prepare to provide quality service.

- Disability Services

IMS will accommodate those with disabilities with culture sensitivity by:

- Treating all members, with or without a disability, regardless of gender, race, sexual orientation, gender identity, religion, cultures, ethnic background, etc., with courtesy and respect. It is important to treat others as you would like to be treated.
- Avoiding patronization and/or pity.
- Speaking directly to the disabled member rather than talking to their companions, aides, or interpreters.
- Conducting due diligence to understand the member and their needs, such as regarding the member's race, religion, preferred language, disability, etc.
- Inquiring about any other alternative/folk treatments.
- Using culturally appropriate courses of inquiry; for example, trying to find out what members have done so far to treat their ailment, such as acupuncture, herbs, acupressure, etc.
- Being aware of body language (verbal/nonverbal cues) while meeting with members and/or physical contact.
- Not making assumptions or decisions about someone's ability to participate in any activity; it is acceptable to ask the person.
- Using patience and active listening for those that have a speech impairment.
- Using clear sentences that use simple and concrete words for members with intellectual disabilities.

There are many other ways to be culturally sensitive to those with disability needs. If there are any other questions, employees should request clarification from their immediate supervisor/Director and/or the Human Resources Department.



- Homelessness Services

IMS understands that there are many contributing factors to homelessness, including poverty, lack of affordable housing and employment opportunities, domestic violence, health and mental health issues, and the effects of trauma. IMS employees and its contracted healthcare physicians and/or affiliates are to treat members that are experiencing homelessness with respect and courtesy, which includes the following:

- Being mindful that homelessness can be secondary to the issues a person is dealing with, such as substance abuse, mental health conditions, developmental disabilities, etc.
- Before providing supportive services, employees and IMS' affiliates and/or healthcare providers should conduct due diligence to understand the person's culture, language and abilities.
- Keeping in mind that a person experiencing homelessness may have limited access to phone services.
- Establishing trust with the member by being honest and clear about services that can/cannot be rendered and being consistent with service follow-through.
- Working with other providers the member may meet, such as community providers including soup kitchens, homeless shelters, libraries, senior centers, culture/ethnic-specific centers, etc.
- Creating a broader list of contacts for the member to utilize, including other family members, friends, and religious counselors, as the member's location changes.
- Providing tangible information and reminders to the member being assisted, along with realistic timeframes and goals.

The items listed above are just some methods used to better serve those that are experiencing homelessness. For any questions, employees should request clarification from their immediate supervisor/director and/or the Human Resources Department.

## **X. Conflict of Interest**

Decisions in the workplace must be made objectively and fairly. If there is a **conflict of interest**, or if other individuals or employees could reasonably believe that there is a conflict of interest, the objectivity and fairness of decisions made could be questioned by colleagues, coworkers, or even the federal and state government. If there is conflict of interest, or perceived conflict of interest, talk to your immediate supervisor/director, the Human Resources Department, and/or the Compliance Department.

### **1. Gifts and Business Courtesies**

Our relationships with our business partners (for example, vendors) are very important. At times, we extend our appreciation to our business partners by giving gifts, especially, during the holidays or special occasions. Our business partners may extend the same appreciation to IMS and its employees. We may accept gifts from our business partners if the following criteria are met:

- The gifts cannot reasonably be an attempt to gain an advantage or be considered a bribe, payoff, or insider deal.
- Gifts offered to members for marketing purposes must be nominal gifts (\$15 or less, or \$75 aggregate per person, per year), provided that the gift is given without discrimination. If a

nominal gift is a chance to receive one large gift or a communal experience (e.g., a concert, raffle, drawing), the total fair market value must not exceed the nominal per person value based on anticipated attendance.

- Nominal gifts may not be in the form of cash or other monetary rebates even if their worth is \$15 or less.

## 2. Members Gifting Employees

At times, members may express their appreciation for the care or treatment they have received by giving an IMS employee a gift. Employees may accept reasonable gifts from grateful members. Perishable items such as food or flowers that cannot be returned may be accepted and shared with others. As an IMS employee, the acceptance of some gifts is prohibited, including:

- Receiving cash or cash-equivalent gifts (for example, checks, gift certificates or cards, coupons and others).
- Accepting a tip for a routine or complimentary service.
- Receiving gifts or entertainment on a regular basis.

## 3. Employees Gifting Others

On occasion, employees may want to show vendors or business partners appreciation by offering a gift, meal, or entertainment, or similar token of appreciation. This is acceptable if:

- Prior authorization is granted from the Managing Principal.
- It does not violate any law or contractual agreements.
- It cannot be construed as a bribe, payoff, deal, or any other attempt to gain advantage.

## 4. The Workplace and Personal Relationships

Employment decisions at IMS must be made based on qualifications and merit. IMS permits relatives and members of the same household to work together if they are qualified candidates. The following relationships are not allowed:

- **Reporting Relationships:** An employee may not report directly or indirectly to a relative or someone that the employee has a personal relationship with. Existing personal relationships, if any, must be approved by the Managing Principal prior to employment with IMS, preferably through written approval.
- **Employment Decisions:** Employees shall not make hiring and/or compensation decisions, including coaching, promoting, or termination of employment for any relatives, members of the same household, or someone with whom an employee has a personal relationship.
- **Performance Feedback:** Employees, supervisors, or directors may not provide performance feedback to any relatives or members of the same household.
- **Working Arrangements:** Relatives or members of the same household working together may create a real or perceived conflict of interest or an unethical or inappropriate situation by being a risk to operations, morale, safety, and security.

## 5. Relatives Who Work for Vendors

Employees of IMS, or anyone associated with IMS, with the authority to direct the use of IMS assets must be careful to avoid any potential conflicts of interest with vendors. Employees should disclose such

matters of potential conflict to their immediate supervisor/director, Human Resources Department, and/or the Compliance Department.

## 6. Other Employment

Employees must comply with all IMS policies. Outside employment, including self-employment, must always be avoided if it interferes or conflicts with IMS' mission, business, or work. Prior approval from the Managing Principal is required to continue such outside employment, to ensure that a conflict of interest does not affect IMS. Generally, employees cannot:

- Be directly involved in the sale of a product or service to IMS while employed by IMS.

Employees must notify management, Human Resources, or the Managing Principal before working as a consultant, independent contractor, representative, or employee of any organization that is a competitor of IMS. If an outside organization that employees are working for becomes a competitor, disclosure is required at that time. Special situations may arise where written disclosure to management, Human Resources, or the Managing Principal is required, such as contracting with a former employer or employee or contracting with an organization that you have worked with in the past. Some exceptions may be granted by management.

## 7. Follow Anti-Kickback Laws

Anti-kickback and Stark laws and similar state laws make it illegal for physicians and other health care providers to knowingly and willfully accept bribes or other kickbacks in return for generating Medicare, Medicaid, or other federal health care business. The Anti-Kickback Law is very complex. Arrangements that involve payments for activities such as recommending or ordering a drug, types of medical equipment, lab tests, and so forth are strictly prohibited. There are severe penalties for violations, including:

- Large monetary penalties
- Exclusion from federal health care programs (like Medicare, Medicaid)
- Imprisonment for up to five (5) years (in the case of Anti-Kickback violations)

# **XI. Government Inquiries and Meeting Expectations**

In the event IMS receives an inquiry, subpoena, or other legal document from a government agency, all management and employees will be notified immediately. It is mandatory to cooperate with government officials. Your management team will ensure that the IMS' response is cooperative and appropriate. Any documentation or information that will be provided to a government agency in response to an inquiry must be coordinated with IMS' legal counsel. The information must be truthful, accurate, complete, and timely.

## 1. Interacting with Government Officials

If an employee or any other IMS workforce member is contacted by a government official, representative, investigator, or any other individual acting on behalf of the government, the employee should immediately:

- Ask to see the individual's credentials and/or proper identification, including a business card and/or employee identification badge, before speaking with the individual any further.

- Immediately contact the Compliance Department, and/or your immediate supervisor/director and/or Human Resources Department.
- Document and list the names and positions of the government representatives/investigators, along with the date and time of the demand, and what is being requested.

Upon receipt of notice and/or information regarding a government investigation, the rest of IMS needs to be made aware of such investigation in an appropriate manner. Directors are to guide and advise their employees on how their employees will cooperate and/or assist the government for needed information.

- **Government Interviews:** If an employee is subject to an interview by a government official, representative, and/or investigator, the employee must always be truthful, cooperative, polite, and professional. The employee may consult with legal counsel and/or the Compliance Department, their immediate supervisor/director, and/or Human Resources if the employee does not know the answer with certainty. The employee may stop the interview or conversation at any time.
- **Demand for Documents:** A government official, representative, investigator, or an individual acting on the behalf of the government may arrive on premises with written authority seeking documents. Usually, this will come in the form of a demand letter, subpoena, or search warrant.
- **Demand Letters and Subpoenas:** if the authorization is a demand letter or subpoena, the employee must request that the government official, representative, investigator, or an individual acting on the behalf of the government wait until the appropriate IMS representative, such as the Compliance Department, their immediate supervisor/director, and/or Human Resources Department, is notified.
- **Search Warrants:** If a valid search warrant and identification of the government official, representative, investigator or individual is presented, employees must understand that the government has the authority to enter the premise, to search for evidence of criminal activity, and to seize those documents/items listed in the warrant.
  - Before the search commences, it is always best to try and request an opportunity to consult with the Compliance Department, and/or your immediate supervisor/director, Human Resources Department, and/or Executive team before responding to any inquiries in connection with the search warrant and/or signing any document presented in connection with the search warrant. However, the request may not be granted by government representatives.
  - No employee shall interfere with the search and must provide the documents or items sought in the warrant.
    - They should request copies of the warrant and the affidavit providing reasons for the issuance of the warrant and should provide the Company with a copy of the warrant immediately, if possible.
    - A list of items/documents and general information should be made of items taken from IMS. Note in as much detail the circumstances, areas, and files that were searched, time periods, and the way the search was conducted.

The employee should always contact the Compliance Department, and/or their immediate supervisor/director, management/Executive team, and Human Resources Department, , so that IMS may

appropriately respond to the demand for documents. Due to the sensitivity and/or confidentiality of some documents, the employee may not have access to them.

## 2. No Gifts for Government Officials

Government officials and their staff are prohibited from accepting anything of value, including services and gifts. It must be reported to the IMS Compliance Department, management team and/or Human Resources Department if employees become aware of gifts being offered to any government officials/staff, or if government officials/staff were invited to any IMS' events.

## 3. Accurate and Timely Reporting to the Government

When reporting to Federal, State, or local government agencies, IMS' reports must be accurate, complete, and timely. Some examples of reporting may include:

- Centers for Medicare and Medicaid Services ("CMS") Parts C and D Reporting Requirements
- Corrective Action Plans (CAPs) – responses to audit and investigations findings
- Hierarchical Conditions Categories (HCCs) – diagnostic and procedural coding requirements of HCCs on risk adjustments

## **XII. Follow Licensing and Certification Requirements**

The health care industry is highly regulated. Licensing and certification requirements for employees must be obtained, as required for their positions, including keeping them up to date.

### 1. Convicted of a Crime

Employees or workforce members who are convicted of a crime in a court of law must disclose this information to their immediate supervisor/director and/or the Human Resource Department as soon as possible. This requirement applies regardless of the type of offense committed, such as a felony or misdemeanor.

## **XIII. Healthcare Sanctions/Exclusion Checks**

The government maintains databases of individuals and entities that have been excluded from participating in federal health care programs. All IMS employees, contractors, and affiliates will be checked against the following databases to determine if they have been excluded from participating in federal health care programs prior to hire or contracting, and on a monthly basis thereafter:

- U.S. Department of Health and Human Services Office of Inspector General's List of Excluded Individuals/Entities
- General Services Administration System for Award Management Excluded Parties List System

A person is "ineligible" when they are currently excluded, debarred, suspended, or convicted of a criminal offense that falls within the scope of 42 U.S.C. §1320a-7(a), but has not yet declared ineligible, and/or is currently excluded on a state exclusion list.

Any employee or contractor that has been added to any these databases must inform their immediate supervisor/director, and the Human Resources Department and Compliance Department as soon as they become aware of it. Any existing or proposed employment, contract, or other association with any individual or entity on these excluded databases will be handled on a case-by-case basis in accordance with the law and IMS policies. All business affiliates and Health Plans will be notified if such occurrence

happens. For further information, please see IMS Compliance Policy and Procedure 70.02.10 and Human Resources Policy and Procedure 70.09.04.

## **XIV. Reporting Suspected Compliance Issues**

Innovative Management Systems is committed to maintaining, as appropriate, confidentiality and anonymity for all individuals reporting compliance issues, real, alleged, or perceived. Employees can seek guidance and report possible violations without fear of harassment, discrimination and/or retaliation. It is better to report something that is suspected than to ignore it. It is best to allow IMS to investigate the matter.

No harassment, discrimination, and/or retaliation is allowed against employees who report concerns that may violate laws, regulations, and/or any IMS policies/procedures in good faith. Employees who intentionally make false allegations/accusations with the purpose of harassing, discriminating, and/or retaliating against another individual, in non-compliance with IMS standards, will be subject to disciplinary actions, up to immediate termination.

### **1. IMS' Compliance Hotline: (1-855-222-1025)**

Employees may try to resolve any issues by meeting with their immediate supervisor/director, Human Resources, and/or management team. If you feel the issue remains unresolved, you may report the issue to the Executive team. In the case that you want to remain anonymous, you may file an anonymous report by calling the Compliance Hotline at 1-855-222-1025.

Any and all potential or actual instances of non-compliance, FWA, or HIPAA breaches must be reported to the Compliance Department. Reports may be filed with the Compliance Department through the following methods:

- **Email:** [Compliance@imsmso.com](mailto:Compliance@imsmso.com)
- **Phone Hotline:** 1-855-222-1025
  - This hotline is available 24 hours a day, 7 days a week
  - Reports can be made confidentially and **anonymously**
- **Online Reporting:** [www.lighthouse-services.com/imsmso](http://www.lighthouse-services.com/imsmso)
  - You can file a report on the web portal **anonymously**
- **Fax:** 1-323-832-8141
- **In-Person:** Reports may be made in person to the IMS Compliance Officer

Providing detailed information will help IMS properly investigate the potential or alleged non-compliance or violation. Purposely making a false report to the Compliance Hotline is a serious violation and employees who do so will be faced with disciplinary actions, up to and including termination.

All reports made will be treated with the utmost discretion and confidentiality.

## **XV. Summary of the Code of Conduct**

- All employees, contractors, and affiliated entities and business associates must abide by all applicable laws and regulations, wherever IMS business is conducted.
- All IMS employees will conduct all business activities with integrity, honesty, respect, empathy, safety, security and confidentiality.
- Employees must not knowingly create, maintain, or submit records, reports, or statements that are inaccurate, false, or misleading. No undisclosed or unrecorded funds or assets can be established. All items of income and expense and all assets and liabilities must be entered into the financial records and must be accurately and adequately described. All reports submitted to governmental authorities must be accurate and complete and all transactions shall be executed in accordance with management’s authorization.
- All confidential information, such as PHI/ePHI, will not be disclosed to unauthorized individuals, and all laws and regulations pertaining to HIPAA must always be followed. IMS employees, contractors, and affiliates will not use confidential information in a way that is not related to IMS business activities during or after their employment. Confidential information cannot be disclosed to competitors, suppliers, or contractors, or to other employees who do not have a legitimate need to know.
- It is important to treat those with diverse backgrounds, cultures, race, ethnicities, disabilities, the same as any other individual employees may encounter daily, regardless of gender, sexual orientation or gender identity. It is important to recognize if any accommodations will be needed in order to provide better services and to conduct business in a culturally competent manner.
- IMS employees must not participate in activities that could create conflicts of interest. A conflict of interest occurs if the activities or responsibilities are detrimental to the interests of IMS or result in improper or illegal personal gain.
- To the extent possible, IMS employees must consult IMS’ Compliance Department, and management/Executive team before interacting with any government official, representatives, and/or investigators. Always verify and document the identification of any government officials, representatives, and/or investigators, along with the interactions and what the government is asking for.
- Any employee or contractor identified as excluded or “ineligible” in the government’s exclusion databases will not be allowed to work for IMS. Anyone who becomes excluded or “ineligible” during their employment or contract must immediately notify their immediate supervisor/manager, and/or the Human Resources Department and Compliance Department.
- Employees who intentionally make false allegations/accusations with the purpose of harassing, discriminating, and/or retaliating against another individual will be subject to disciplinary actions, up to immediate termination.




## **XVI. IMS Employee Resources**

Should you have any questions, please refer to any of the resources listed below for additional guidance:

- IMS Departmental Policies and Procedures:
  - X:\!IMS Policy and Procedures [ALL EMPLOYEES]
  - Y:\!IMS Policy and Procedures [ALL EMPLOYEES]
  - S:\!IMS Policy and Procedures [ALL EMPLOYEES]

- IMS Employee Handbook
  - Your supervisor/director and/or management team
  - The Human Resources Department
  - The Compliance Department
  - Executive Team
- 

Board of Director Reviewed and Approved:

|              |  |                 |
|--------------|--|-----------------|
| John Chung   | Sign  | Date 10/09/2022 |
| Wonny Sung   | Sign  | Date 10/09/2022 |
| Lee Suyenaga | Sign  | Date 10/10/2022 |