Provider Oversight & Compliance Orientation and Training

2026

INTEGRATED
HOME CARE SERVICES

Provider Oversight & Compliance Orientation

Welcome to the Integrated Home Care Services' (IHCS) family of providers in the delivery of home care services. We are pleased to have you in our network and look forward to partnering with you in the provision of high-quality home care services.

This Onboarding Presentation is presented by
IHCS Vendor Delegation Monitoring Team/Provider Relations Team

Ongoing and refresher training will be conducted throughout each year

If you have any questions or need additional assistance, please do not hesitate to contact the Provider Relations team at providerservices@ihcscorp.com.

TABLE OF CONTENTS

PROVIDER OVERSIGHT AND SUPPORT

PROVIDER SATISFACTION & VENDOR SCORE CARDS

PROVIDER SATISFACTION SURVEYS

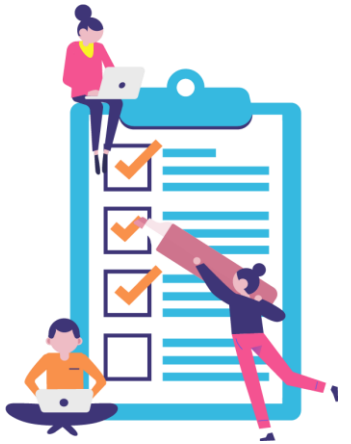
Satisfaction Surveys will be sent electronically to all IHCS Providers quarterly via SurveyMonkey.

It is important that our downstream providers share their experience and overall satisfaction with IHCS with us.

VENDOR SCORE CARDS

IHCS randomly selects 10 downstream providers each month to “score” on their overall performance.

- **Acceptance of Referrals/TAT’s/UM Compliance**
- **Demonstrated Clinical Proficiency**
- **MedTrac Documentation (NOMNC’s)**
- **Patient Satisfaction/Member Complaints**
- **Credentialing Profile/Compliance Practices**
- **Claims Accuracy**



IHCS PROVIDER RELATIONS DEPARTMENT

Susan Klarner – VP of Network Development

Jose Gonzalez – Director, Provider Relations

Manuel Bustillo – Manager, Provider Engagement

Cynthia Leon – EVV,PDN Provider Relations Liaison

Allison Fernandez – Provider Relations Liaison

Yane Mirabal – Provider Relations Liaison

Luis Reig – Provider Engagement Specialist

Sebastian Pino – Provider Relations Analyst

Ronald Ramjeawan – Physician Relations Liaison

Traicy Carrasco – Provider Relations Specialist

Shellyann Burton – Provider Relations Specialist

Jessica Burgos – Provider Relations Specialist

Dwayne Sinclair – Provider Engagement Specialist

Ronald Gutierrez – Provider Relations Specialist

Mollie Ruffolo – Provider Engagement Specialist

Antonio Milton – Provider Engagement Specialist

Email: Providerservices@ihcscorp.com
Phone: 844-215-4264 *Ext 2546*
Fax: 954-624-8731

IHCS CORPORATE COMPLIANCE PROGRAM
&
CODE OF CONDUCT

- 2026 -

INTRODUCTION

All persons who provide health or administrative services to Medicare enrollees must satisfy General Compliance Training, as well as Fraud, Waste, and Abuse (FWA) training requirements.

Providers who have met the FWA certification requirements through enrollment into the Medicare program or are accredited as a Durable Medical Equipment, Prosthetics, Orthotics and Supplies (DMEPOS) provider are deemed to have met the FWA training and education requirement, but not the general compliance training.

Compliance is EVERYONE'S responsibility!

As an individual who provides health or administrative services for Medicare enrollees, every action you take potentially affects Medicare enrollees, the Medicare program, or the Medicare trust fund.

CORPORATE COMPLIANCE PROGRAM AND CODE OF CONDUCT 

Compliance
m & Code of Conc

WHAT IS NONCOMPLIANCE?

Non-compliance is a conduct that does not conform to the law, and Federal health care program requirements, or to an organization's ethical and business policies.

- Credentialing
- Appeals & Grievance Review
- Claims Processing
- Ethics
- HIPAA
- Marketing & Enrollment
- Conflicts of Interest
- Financial Incentives
- Beneficiary Notices
- Agent / Broker
- Documentation Requirements
- Quality of Care
- Formulary Administration

Medicare Parts C & D High Risk Areas *

2026 - IHCS Medicare Parts C & D General Compliance Training

Medicare Parts C
› Compliance Trair

HOW CAN I REPORT POTENTIAL NONCOMPLIANCE?

Employees of an MA, MA-PD, or PDP Sponsor

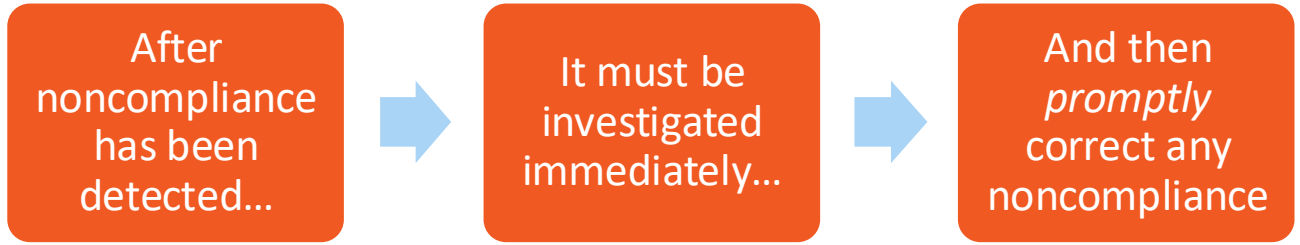
- Call the Medicare Compliance Officer
- Make a report through the Website
- Call the Compliance Hotline

FDR Employees

- Talk to a Manager or Supervisor
- Call your Ethics/Compliance Help Line
- Report through the Sponsor

Beneficiaries

- Call the Sponsor's compliance hotline
- Make a report through Sponsor's website
- Call 1-800-Medicare



Correcting Noncompliance

- Avoids the recurrence of the same noncompliance
- Promotes efficiency and effective internal controls
- Protects enrollees
- Ensures ongoing compliance with CMS requirements

HOW DO I KNOW THE NONCOMPLIANCE WON'T HAPPEN AGAIN?

Once noncompliance is detected and corrected, an ongoing evaluation process is critical to ensure the noncompliance does not recur.

Monitoring activities are regular reviews which confirm ongoing compliance and ensure that corrective actions are undertaken and effective.

Auditing is a formal review of compliance with a particular set of standards (e.g., policies and procedures, laws, and regulations) used as base measures.

KNOW THE CONSEQUENCES OF NONCOMPLIANCE

Your organization is required to have disciplinary standards in place for noncompliant behavior.

For example, IHCS Policy 131 **prohibits the practice** of providing financial incentives to staff members, practitioners, or providers based on their limiting member utilization of health care services. All IHCS employees and downstream providers will sign an attestation upon onboarding and annually thereafter.

Those who engage in noncompliant behavior may be subject to any of the following:

WHO GOVERNS COMPLIANCE?

Social Security Act: Title 18

Code of Federal Regulations*:

42 CFR Parts 422 (Part C) and 423 (Part D)

CMS Guidelines:

Manuals

HPMS Memos

CMS Contracts:

Private entities apply and contracts are renewed/non-renewed each year

Other Sources:

OIG/DOJ (fraud, waste, and abuse [FWA])

HHS (HIPAA privacy)

State Laws:

Licensure

Financial Solvency

Sales Agents

* 42 C.F.R. **§§ 422.503(b)(4)(vi) and 423.504(b)(4)(vi)**

ADDITIONAL RESOURCES

For more information on laws governing the Medicare program and Medicare noncompliance, or for additional healthcare compliance resources please see:

- Title XVIII of the Social Security Act
- Medicare Regulations governing Parts C and D (42 C.F.R. §§ 422 and 423)
- Criminal False Claims Statute (18 U.S.C. §§ 287,1001)
- Anti-Kickback Statute (Physician Self-Referral Law) (42 U.S.C. § 1395nn)
- Exclusion entities instruction (42 U.S.C. § 1395w-27(g)(1)(G))
- The Health Insurance Portability and Accountability Act of 1996 (HIPAA) (Public Law 104-191)

(45 CFR Part 160 and Part 164, Subparts A and E)

- OIG Compliance Program Guidance for the Healthcare Industry:

http://oig.hhs.gov/compliance/compliance-guidance/index.asp

Preventing Fraud, Waste, & Abuse

The prevention of fraud, waste and abuse is the responsibility of every Integrated Home Care Services team member and business partner. Fighting the inappropriate loss of Medicare and Medicaid healthcare dollars through fraud, waste, abuse, and other improper payments is a priority for Integrated Home Care Services.

Home health agencies and durable medical equipment (DME) providers offer services and supplies vulnerable to fraud. Integrated Home Care Services plays a significant role in the fight against fraud, waste, and abuse in Medicare and Medicaid home health, home infusion, and DME. While the specific requirements for home health, home infusion and DME can vary from state to state, all States require furnished services to be medically necessary. Integrated Home Care Services and its team members and business partners have a responsibility to know the rules for home health, home infusion, and DME services as required by Medicare and State Medicaid programs.

- Examples of home health fraud include attesting falsely to the medical necessity of home health services, accepting compensation for ordering specific services irrespective of medical necessity, or physicians signing plans of care for beneficiaries not under their care.

- Examples of DME fraud, waste, and abuse include physicians selling medically unnecessary prescriptions and DME companies recruiting patients and then billing Medicaid for more expensive equipment than what is delivered.

Improving performance in key areas would save 100,000 to 150,000 lives and $50 billion to $100 billion annually.

The Commonwealth Fund Commission on a High-Performance Health System.

The **Patient Protection and Affordable Care Act**, more commonly known as the **Affordable Care Act**, enacted in 2010, provides tools to prevent, detect and take strong enforcement action against fraud in Medicare, Medicaid and private insurance.

The **Affordable Care Act (ACA)** seeks to improve anti-fraud and abuse measures by focusing on prevention rather than the traditional "pay-and-chase" model of catching criminals after they have committed fraud.

There are four principal ways the ACA seeks to make changes:

- More money to prevent and fight fraud
- Better screening and compliance
- New penalties
- Better data sharing

HOME HEALTH FRAUD

To help reduce opportunities for fraud in home health, the ACA:

- Requires physicians who order home health services to be enrolled in Medicare.

- Requires a face-to-face encounter within 90 days prior to the home health start of care date.

HOW IHCS CAN PREVENT FRAUD, WASTE, AND ABUSE

Integrated Home Care Services plays an important role in promoting integrity to minimize and prevent fraud, waste, and abuse in Medicare, Medicaid and private insurance programs.

The following are key points for providers to remember.

Confirm eligibility: Verify the eligibility status of patients at the time of service.

Include identifiers: If required by the State when ordering services or supplies, the ordering provider's signature and National Provider Identifier (NPI) should be included on the CMN or other prior authorization form.

Order appropriately: Order according to the medical needs of the beneficiary within the limits set by the State/Medicare.

Maintain organized records: Keep patient records organized and up-to-date and confirm that the patient's condition warrants the service requested in the CMN or prior authorization request.

Educate staff: Integrated Home Care Services should educate staff on the issues and schemes that constitute fraud, waste, and abuse.

Practice within scope: Always document the medical necessity of the service(s) ordered. If a medically unnecessary service is billed or if the documentation does not justify medical necessity, it may be considered a "false claim."

Protect yourself: Be on the alert for other professionals who may make inappropriate requests, such as a "quick signature" on a document for a patient never seen, asking for additional patient services because of convenience rather than medical necessity, asking for beneficiary medical identifiers when there is no specific need, or offering to provide remuneration for beneficiary referrals.

QUALITY OF CARE AND PATIENT SAFETY

At Integrated Home Care Services, we understand that our patients are unique individuals. We provide care in a safe, effective and efficient manner.

To encourage this effort, our clinical quality improvement team builds and designs systems and processes incorporating best practices in caring for patients.

- We follow up with patients and other caregivers to create a safe environment and improve communication.
- We encourage anyone on any team to stop a process if he or she thinks it is incorrect.
- We maintain standards for licenses and credentials for caregivers who work in all locations.
- We report unanticipated outcomes to a supervisor and prepare for appropriate follow-up and communication with the patient and family.

PATIENT RIGHTS

We are committed to informing our patients of their rights and to protecting their rights.

We deliver high-quality care when we respect and support patients and their loved ones and give them information to make decisions regarding the care they are offered.

- We provide each patient with a written statement of patient rights and a notice of privacy practices.
- We provide kind and respectful care no matter a patient's personal values and beliefs, age, sex, race, color, religion, disability, national origin, ability to pay, or any other category protected by state or federal law.
- We seek to resolve patient complaints promptly and to provide contact information so patients can report grievances.
- We seek to follow a program by which all patients have the right to be free of any coercion as to selection of a provider, health plan or medical procedure.

CONFIDENTIALITY OF PATIENT INFORMATION

The information we create, use and disclose while taking care of our patients is sensitive and personal. We are committed to keeping all patient information protected and secure.

We receive training to understand the various requirements Integrated Home Care Services must meet to comply with HIPAA and to protect our patients' information.

- We only discuss patients and their care with authorized persons in appropriate places and with low voices.
- We verify the identity of the person requesting a copy of a patient record and require a completed authorization to release information.
- We access only the appropriate amount of patient information we need to do our jobs.
- We provide individuals with timely access to their healthcare information.
- We provide patients with our Notice of Privacy Practices.
- We hold business partners to the same standards when they conduct business on our behalf.

LICENSE, CERTIFICATION, E-VERIFY AND EXCLUDED PERSONS

The Integrated Home Care Services purpose and values guide the requirements we set for our team members. We are committed to ensuring that only individuals who are eligible to participate in federal healthcare programs work at Integrated Home Care Services.

We ensure that care providers have valid licensure, certification, registration or other credentials.

- We have a monthly process to screen all team members, network providers, and business partners with access to member information to ensure that Integrated Home Care Services does not employ or contract with persons or entities excluded from Medicare, Medicaid or any federal health care program.

- We require all team members and business partners to disclose immediately if they are excluded from Medicare, Medicaid or any federal health care program.

- The Vendor shall comply with **Section 274A of the Immigration and Nationality Act**. IHCS will consider the employment by any contractor of unauthorized aliens a violation of this Act. If your agency knowingly employs unauthorized aliens, such violation shall be cause for unilateral cancellation of your Provider Contract. Your agency shall be responsible for the enforcement of this compliance protocol.

HIPAA PRIVACY & SECURITY TRAINING FOR ALL PROVIDERS, COVERED ENTITIES, AND BUSINESS ASSOCIATES

- 2026 -

INTRODUCTION

Integrated Home Care Services (IHCS) or ("Integrated") is committed to a culture of ethical business practices and compliance.

Integrated's success as an industry leader is based on realizing our mission through policies and procedures
The purpose of this training is to provide an overview of the Health Insurance Portability and Accountability Act (HIPAA) to our Network Providers.

Additional training may be available to address specific HIPAA requirements for your SBU or area of responsibility.

WHAT IS YOUR ROLE?

HIPAA permits providers, insurance companies, and other healthcare entities and business associates to exchange information necessary for treatment, payment, and healthcare business operations.

Based on inappropriate actions or breaches in confidentiality by downstream provider employees, your company or employees can be held liable and may be subject to sanctions for violations.

Downstream Provider employees having access to IHCS Personal Health Information (PHI) will need to ensure compliance with internal policies and federal regulations to ensure all confidential information is treated with the highest level of integrity and respect for the confidentiality of the information.

IHCS is committed to holding all Network Providers actions in accordance with HIPAA regulations.

Vendors must also be able to demonstrate how security incidents or breaches are managed.

Remember, Integrated must be immediately notified of a breach as part of regulatory and contractual requirements.

In Addition:

- Vendors must ***separate IHCS data*** from other clients.
- Access to vendor databases, systems or reports ***must be role-based*** and as needed.
- Access reviews for privileged data should be quarterly **OR** twice a year for non-privileged data. Attestation of access reviews must be signed and saved for future audits.
- Methods to ***limit access*** and protect personal health information and personally identifiable information such as Social Security Numbers must be documented.
- Privacy ***risk assessment*** should be performed at least annually to proactively identify risks that could impact yours and Integrated's business.

TRAINING OBJECTIVES

- Define the provisions of HIPAA
- Recognize and understand the importance of complying with HIPAA
- Understand and be able to identify examples of PHI
- Identify the actions needed to secure PHI
- Understand consequences for not complying with HIPAA
- Identify your Agency's responsibilities for reporting privacy and security incidents to IHCS

This Privacy Information Security Training is part of an evaluation of downstream vendor policies, procedures, and standards with respect to Business Associate Agreements. Elements that will be reviewed in this training focus on key risk areas that may heighten IHCS exposure to security incidents or breaches. How vendors manage regulatory oversight and what control mechanisms are in place to prevent, detect, and correct non-compliance will be validated.

WHAT IS HIPAA AND WHO MUST COMPLY?

The Health Insurance Portability & Accountability Act, known as HIPAA:

- Permits the disclosure of health information needed for patient care and other important purposes
- Provides federal protection for individually identifiable health information held by covered entities and their business associates
- Gives patients rights with respect to how their information is handled

The requirements of HIPAA and PHI requirements align with Integrated's values on how we treat our customers and want you to as well!

Two types of organizations must comply with HIPAA:

- **Covered Entities** which include healthcare providers, like Integrated 's Home Health, DME and Home Infusion businesses, health plans and healthcare clearing houses
- **Business Associates** are companies or individuals who perform services for Covered Entities and who have access to Protected Health Information received from Covered Entities
- A **BAA or Data Sharing Agreement** must be signed between the provider and IHCS at the onset of business.

PROTECTED HEALTH INFORMATION (PHI)

The Privacy Rules applies to a class of information known as Protected Health Information (PHI).

PHI is information held or transmitted by a Covered Entity or its Business Associate that relates to:

- An individual's physical or mental health
- The provision of healthcare to the individual
- Payment for the provision of healthcare for the individual where the information gives a reasonable basis for identifying the individual

Examples of PHI include:

- Name of individual
- Postal or email address
- Telephone or fax number
- Social Security number
- Date of birth
- Health, claims and assessment related information
- Credit card number
- Medical record
- Policy number
- Medical device identifier and serial number
- Financial account information
- Payment information

We must comply with the requirements to report and mitigate any unauthorized use or disclosure of PHI.

MINIMUM NECESSARY STANDARD

- When using, disclosing or requesting PHI, agencies like yours must make reasonable efforts to limit information to the minimum amount necessary to accomplish the intended purpose of the use, disclosure, or request.

- The minimum necessary standard applies to all documented, verbal and electronic PHI data.

- It is a requirement of all Integrated employees and contracted providers to uphold this commitment and requirement to the regulations.

- Providing quality and outstanding care for our customers is a top priority to Integrated.

HIPAA PRIVACY

- Gives individuals rights to control and directly access their own health information.
- Requires your agency to protect every insured's information from unauthorized access, use, or disclosure.
- Limits uses and disclosures of PHI only to those that are authorized by the individual in writing, contractually allowed, or required by law.

LEGALLY & PERSONALLY AUTHORIZED INDIVIDUALS

- **Personal Representatives** are legally authorized by the individual to access PHI and exercise their individual rights
- **Authorized Individuals** are designated to have access to PHI to assist the individual, but do not have decision making authority
- **Certain agency employees** are designated with the authority to have PHI in performing the duties of their position

NOTICE OF PRIVACY PRACTICES

The Notice of Privacy Practices:

- Contains a description of permissible uses and disclosures of PHI.
- States that an insured's written authorization is required for any use or disclosure of PHI outside of:
  - Treatment
  - Payment, or
  - Health Care Operations
- Explains covered entity's duties to protect health information privacy.

Outlines HIPAA Individual Rights Requests including the right to:

- Request an amendment of incorrect PHI
- Request an accounting of disclosures of PHI
- Request confidential communications
- File a complaint or an appeal
- Request restrictions
- Request information about privacy policies

HIPAA SECURITY RULE

HIPAA regulations define the standards required for securing PHI

- HIPAA requires organizations to ensure that all PHI, regardless of its form (e.g., paper, electronic files, email reports, spoken), are secure.
- All your employees who trust, PHI must follow the administrative, technical, and physical safeguards to protect the confidentiality, integrity, and availability of PHI.
- Securing PHI ensures we keep our customers' trust, and it also reduces the risk of incidents or HIPAA violations.
- HIPAA violations can have legal consequences and sanctions against your agency!

TECHNICAL SAFEGUARDS

The HIPAA Security Rule requires Integrated to establish and implement administrative safeguards to manage the privacy of PHI.

IT groups at Integrated ensure appropriate systems are in place to safeguard data internally and externally with your agency's office.

Integrated has established its own security policies and procedures in the use, storage, disclosure, and disposition of PHI data that your agency must comply with.

Note: It is the recommendation of IHCS that downstream providers invest in Cyber Insurance to protect themselves and IHCS from cyber incidents….

DATA SECURITY

- Your agency should establish data security practices including:
  - Requiring passwords that consist of a combination of characters, such as upper and lowercase letters, special characters and numbers.
  - Setting laptop or mobile device screensavers to require a password and appear automatically when the device is not in use.
  - Prohibiting individuals from sharing passwords with anyone, including family, friends, or coworkers.
  - Encrypting PHI stored on portable devices (e.g., laptops, mobile phones) and PHI that is transferred electronically (e.g., through e-mail and other online services).

DATA ACCESS & USE INSTRUCTIONS

Your responsibility is to:

- Follow Integrated's security policies whenever accessing, using, or disclosing PHI.
- Only access PHI if you have a legitimate need to do so.
- Limit the use and disclosure of PHI to the minimum necessary.

SECURITY, STORAGE & DISPOSAL

Facilities and Work Areas

- Ensure that your facilities and work areas containing PHI are secure
- Ensure that anyone entering a controlled area scans their badge or ID (*if applicable*)
- Do not allow anyone to follow you or "piggyback" into an area without swiping their access badge (*if applicable*)

Storage and Disposal

- Store PHI in secure areas
- Dispose of documents and electronic media containing PHI in secured containers or by shredding
- Keep mobile devices containing PHI secure

LOST OR STOLEN LAPTOPS OR COMPANY PHONES

In the event an agency's team member's laptop is lost or stolen, the loss must be immediately reported to IHCS.

An investigation needs to be conducted to determine the risk of the data and potential use of the data in violation of HIPAA regulations.

To avoid theft of agency equipment all employees should demonstrate appropriate judgment in safeguarding not only the physical property of the company, but also the confidential information stored on the computer, or phone.

WORK AREA INSTRUCTIONS

- Keep PHI out of view from the public on desks, copiers/fax machines, whiteboards, etc.
- Make certain you quickly remove any PHI from printers and surrounding areas.
- Be aware of your surroundings when discussing or handling PHI. Do not discuss PHI in areas where unauthorized individuals can hear information being discussed.
- Discussions about any IHCS client information should be limited in a needs to know capacity, and specific information must not be included in any informal conversations with other employees, friends or family members.

ENFORCEMENT & PENALTIES

HIPAA has specific penalties for failing to protect PHI. Any improper release, acquisition, use, or disclosure of PHI is considered a privacy or security incident or “breach”.

Carelessness or unintentional breaches not only violate individuals' privacy —and trust in Integrated —but also have serious consequences ranging from agency actions including warnings, suspensions or termination of contract.

Monetary penalties from the government exist to provide consequences for those who violate HIPAA rules and regulations.

HIPAA requires a duty to report voluntary disclosure of violations.

US Department of Justice (DOJ), Office of Civil Rights (OCR), Centers for Medicare & Medicaid Services (CMS),Office of Inspector General (OIG), Federal Trade Communications (FTC), various State Departments of Insurance, and State Attorneys General.

HITECH ACT

The **Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009** was created to incentivize the healthcare industry to adopt Electronic Health Record Systems. Electronic records have a greater risk of being compromised, so increased safeguards were needed.

The HITECH Act:

- Strengthens the elements of the Security Rule
- Requires audits to ensure compliance
- Authorizes the State's Attorney General to bring actions under HIPAA
- Dramatically increases penalties for non-compliance

NON-COMPLIANCE

For Integrated and its downstream providers such as you, failing to comply with HIPAA as amended by HITECH could lead to some or all of the following:

- Disciplinary action for our businesses and the individual
- Possible criminal penalties with up to 10 years in prison
- Personal fines up to and may exceed $250,000
- Sanctions against Integrated and its provider network agencies resulting in amplified scrutiny.

BREACH

All privacy and security incidents involving PHI need to be investigated.

Your employees are responsible for reporting suspect actions immediately —no matter how minor they may appear —through our incident reporting process.

Reporting incidents immediately can help prevent simple mistakes from turning into catastrophic breaches.

The **HIPAA Breach Risk Assessment Tool** can be completed if you suspect a breach has occurred; it is an easy-to-use tool to measure the severity of the breach.

Complaints or inquiries from Federal or State regulators in the last two (2) years should be logged, tracked, and reported to IHCS. Corrective action plans on security incidents or breaches should be shared with IHCS as part of regulatory and contractual requirements.*

IHCS HIPAA
:h RIsk Assessment

YOUR AGENCY'S RESPONSIBILITIES

Everyone who handles or maintains PHI while doing their job must comply with HIPAA.

If you become aware of any PHI being misdirected via mail, email, fax, verbally or otherwise, you are obligated to gather and report all relevant details to Compliance.

By following the HIPAA Privacy and Security Rules, you support Integrated's commitment to ensure the privacy and security of patient information.

You also help protect both yours and Integrated's reputation and avoid costly penalties!

HIPAA COMPLIANCE

If you have any questions regarding HIPAA compliance or your role in enforcing HIPAA rules and regulations, contact your manager, a member of the IHCS Compliance Team or your own HR Generalist.

Inform an IHCS Compliance Team member of any HIPAA disclosure or any suspected unlawful practice HIPAA grants whistleblower protection from discrimination and retaliatory actions to anyone who initiates or participates in a privacy complaint process.

COMPLIANCE CONTACT INFORMATION

You are obligated to report any and all HIPAA disclosures involving IHCS data to:

- IHCS 24-Hour Compliance Hotline - 954-381-7954 or compliance@ihcscorp.com
- Compliance Fax Line - 844-215-4265
- HIPAA, Complaints and Fraud referrals via compliance@ihcscorp.com

SUMMARY

Integrated wants all vendor agencies to be aware of HIPAA requirements. If there are requirements that are specific to your role or SBU, additional training can be provided.

Following is a review of the key points covered in this training:

- HIPAA requires Integrated and her Business Associates to keep PHI private and secure for its customers.
- PHI is health-related information that can be used alone or in combination with other information to identify an individual.
- PHI can only be used and disclosed to the minimum necessary or need to know.
- Unauthorized access of PHI has severe consequences to all employees.
- Your employees are required to understand and comply with Integrated's policies and procedures as they relate to HIPAA and the handling of PHI.
- Your employees have a responsibility and obligation to identify and report suspected privacy and security incidents and violations.

HIPAA Administrative Simplification

Regulation Overview of 45.CFR 162.923

General Rule: When a covered entity conducts a transaction for which a standard has been adopted with another covered entity (or within the same covered entity) using electronic media, the covered entity must conduct the transaction as a standard transaction. Conducting a transaction as a "standard transaction" includes compliance with the standard as well as affiliated operating rules, code sets, and unique identifiers for the particular transaction.

Use of a Business Associate: If a covered entity uses a business associate, as defined in 45 CFR § 160.103, to conduct all or a portion of a transaction for which a standard has been adopted, the covered entity must require their business associate and any of the business associate's agents or subcontractors to comply with all applicable requirements.

Trading Partner Agreements: A covered entity cannot enter into a trading partner agreement that would: (a) change the definition, data condition, or use of a data element or segment in an adopted standard or operating rule; (b) add any data elements or segments to the maximum defined data set; (c) use any code or data elements marked "not used" or that are not in a standard; or (d) change the meaning or intent of a standard. Covered entities may not agree to conduct transactions with each other that violate the adopted standards. The requirement to conduct transactions as standard transactions as described in 45 CFR§162.923(a) overrides any agreements to conduct transactions otherwise.

For more information on the complete Administrative Simplification Overview, please open the attached fact sheet document.

HIPAA
trative Simplificati

OIG SCREENING

All **new hire direct patient care employees when applicable** will, prior to being hired, have the following background checks completed:

- Criminal Background Record (AHCA Level II Screening)
- Office of Inspector General (OIG) (May be performed by outside agency)
- National Sex Offender Registry /OFAC/SAM
- MVR (If operating a company vehicle in the course of doing business at time of hire and annually)

All **new hire employees who have access to patient records** will, prior to being hired, have the following background checks completed:

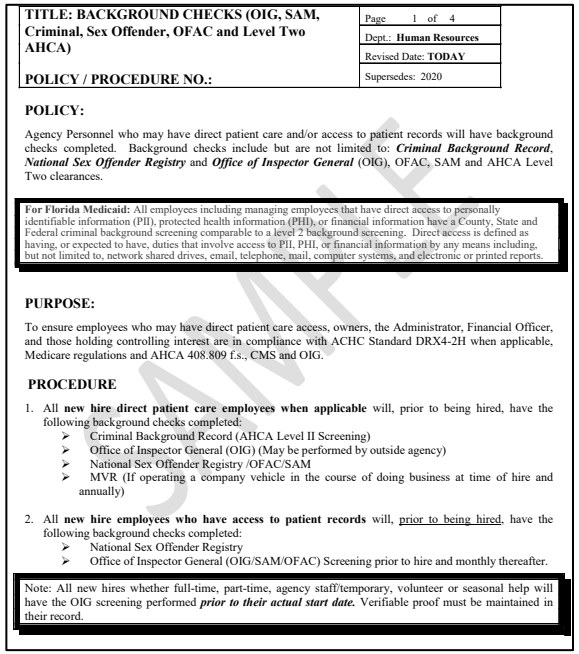
- National Sex Offender Registry
- Office of Inspector General (OIG/SAM/OFAC) Screening prior to hire and monthly thereafter.

All employees will have an Office of Inspector General (OIG, OFAC, OPT-OUT and SAM) **check once a month thereafter.**

All ***direct patient care*** employees will have a Criminal Background Record AHCA Level Two check completed every five (5) years per AHCA guidelines. 408.809

Any employee, candidate, provider or vendor who is identified as being on any of the above regulatory "Exclusion Lists" will be reported to the Director of Compliance or Administrator for subsequent action as required within 24 hours of discovery. (Don't forget to report it to IHCS Compliance Department)

The Company may utilize Compliance Resource Center (or same/similar service) to run the OIG, SAM and OFAC report on a monthly basis. (This list can be provided to IHCS for monthly proof)



TITLE: BACKGROUND CHECKS (OIG, SAM, Criminal, Sex Offender, OFAC and Level Two AHCA)

Page 1 of 4
Dept.: **Human Resources**
Revised Date: **TODAY**
Supersedes: 2020

POLICY / PROCEDURE NO.:

POLICY:

Agency Personnel who may have direct patient care and/or access to patient records will have background checks completed. Background checks include but are not limited to: ***Criminal Background Record***, ***National Sex Offender Registry*** and ***Office of Inspector General*** (OIG), OFAC, SAM and AHCA Level Two clearances.

For Florida Medicaid: All employees including managing employees that have direct access to personally identifiable information (PII), protected health information (PHI), or financial information have a County, State and Federal criminal background screening comparable to a level 2 background screening. Direct access is defined as having, or expected to have, duties that involve access to PII, PHI, or financial information by any means including, but not limited to, network shared drives, email, telephone, mail, computer systems, and electronic or printed reports.

PURPOSE:

To ensure employees who may have direct patient care access, owners, the Administrator, Financial Officer, and those holding controlling interest are in compliance with ACHC Standard DRX4-2H when applicable, Medicare regulations and AHCA 408.809 f.s., CMS and OIG.

PROCEDURE

1. All **new hire direct patient care employees when applicable** will, prior to being hired, have the following background checks completed:
   - Criminal Background Record (AHCA Level II Screening)
   - Office of Inspector General (OIG) (May be performed by outside agency)
   - National Sex Offender Registry /OFAC/SAM
   - MVR (If operating a company vehicle in the course of doing business at time of hire and annually)
2. All **new hire employees who have access to patient records** will, prior to being hired, have the following background checks completed:
   - National Sex Offender Registry
   - Office of Inspector General (OIG/SAM/OFAC) Screening prior to hire and monthly thereafter.

Note: All new hires whether full-time, part-time, agency staff/temporary, volunteer or seasonal help will have the OIG screening performed ***prior to their actual start date.*** Verifiable proof must be maintained in their record.

SAMPLE

Click for embedded sample policy

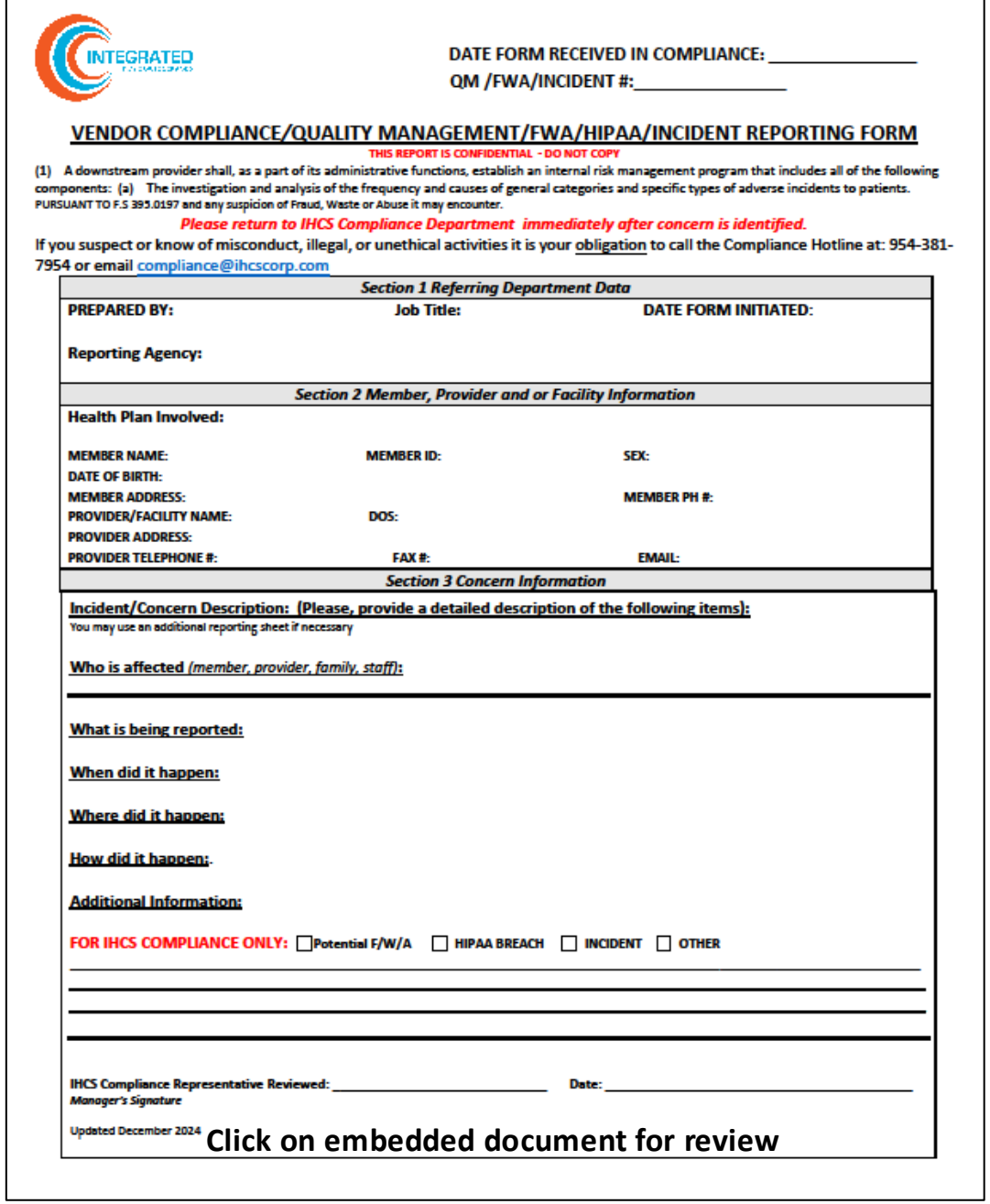
RISK MANAGEMENT
&
INCIDENT REPORTING

Vendor Compliance / Quality Management / FWA Concern Report Form

A downstream provider shall, as a part of its administrative functions, establish an internal risk management program that includes all of the following components:

The investigation and analysis of the frequency and causes of general categories and specific types of adverse incidents to patients. PURSUANT TO F.S 395.0197 and any suspicion of Fraud, Waste, or Abuse it may encounter.

Please contact Provider Relations at Providerservices@ihcscorp.com for the form.



INTEGRATED

DATE FORM RECEIVED IN COMPLIANCE: _____
QM /FWA/INCIDENT #:_____

VENDOR COMPLIANCE/QUALITY MANAGEMENT/FWA/HIPAA/INCIDENT REPORTING FORM

THIS REPORT IS CONFIDENTIAL - DO NOT COPY

(1) A downstream provider shall, as a part of its administrative functions, establish an internal risk management program that includes all of the following components: (a) The investigation and analysis of the frequency and causes of general categories and specific types of adverse incidents to patients. PURSUANT TO F.S 395.0197 and any suspicion of Fraud, Waste or Abuse it may encounter.

Please return to IHCS Compliance Department immediately after concern is identified.

If you suspect or know of misconduct, illegal, or unethical activities it is your obligation to call the Compliance Hotline at: 954-381-7954 or email compliance@ihcscorp.com

Section 1 Referring Department Data

PREPARED BY: Job Title: DATE FORM INITIATED:

Reporting Agency:

Section 2 Member, Provider and or Facility Information

Health Plan Involved:

MEMBER NAME: MEMBER ID: SEX:
DATE OF BIRTH:
MEMBER ADDRESS: MEMBER PH #:
PROVIDER/FACILITY NAME: DOS:
PROVIDER ADDRESS:
PROVIDER TELEPHONE #: FAX #: EMAIL:

Section 3 Concern Information

Incident/Concern Description: (Please, provide a detailed description of the following items):
You may use an additional reporting sheet if necessary

Who is affected *(member, provider, family, staff)*:

What is being reported:

When did it happen:

Where did it happen:

How did it happen:

Additional Information:

FOR IHCS COMPLIANCE ONLY: ☐ Potential F/W/A ☐ HIPAA BREACH ☐ INCIDENT ☐ OTHER

IHCS Compliance Representative Reviewed: _____ Date: _____
Manager's Signature

Updated December 2024

Click on embedded document for review

POLICY

The Company maintains a proactive approach to ensuring the safety of all employees and patients served.

The Company maintains a system to identify, respond, report and reconcile untoward and/or unusual events when they occur.

Such events are known as **INCIDENTS** and defined as follows:

- ***An incident is unusual event involving company personnel, patient, family/caregiver or property.***
  - *The event is considered unusual if the result was unintended, undesirable, and/or unexpected.*

- ***An incident is also any happening that is not consistent with the routine operation of the company or the routine care/service of a patient.***
  - *It may involve an actual event or a potential event, if that event was determined to be likely to occur in the considered opinion of the staff member who reports the incident.*

State Law under §641.55, F.S.: Internal Risk Management (RM) Program, requires all HMO employees complete RM Program training and comprehend Program objectives, grievance procedures, incident reports, and reporting requirements, including Code15. As a TPA, IHCS joins our health plan partners in these endeavors.

***OIR-** Office of Insurance Regulation*

***AHCA-** Agency for Healthcare Administration*

***AAAHC-** Accreditation Association for Ambulatory Health Care, Inc*

At a minimum, the following events are reportable incidents:

- Loss or breakage of any patient owned property or materials;
- Malfunction and/or failure of any equipment or supplies leased or sold by the company;
- Adverse Drug Reaction involving any U.S.P. Medical Oxygen or infusion prepared or delivered by the company;
- Failure to manufacturer, produce, maintain U.S.P. Medical Oxygen or drugs in accordance with law, regulation, and accepted standards of practice;
- Failure to provide product(s) and/or service(s) as authorized;
- Providing medical gases, regulated medical equipment, or drugs without benefit of a physician's order;
- Any compromise of Building Integrity that threatens personnel or agency operations;
- Any event involving a motor vehicle owned or leased by your organization;
- Any event that involves the endangerment of a patient, caregiver and/or staff member;
- Any injury to a patient that results from the use or misuse of equipment, supplies or drugs provided by this organization;
- Any injury to a staff member that occurred while that individual was "on duty" for this organization;
- Any untoward outcome that results from the use/misuse of any equipment, supply, or medical gas provided by this company;
- Failure of system(s) designed to preserve and/or protect the confidentiality of patients or staff;
- All patient or employee accidents/injuries regardless of medical follow-up activity;
- Any other event that is perceived to have an actual or potential adverse impact to staff, patients and/or company operations.

Prevention Tips for Providers

- Do not attempt any procedure without adequately training.
- Maintain a strong, positive rapport with patients.
- Make sure all information accurate/recorded (initialed), tracked, and communicated to patient with documentation.
- Document how patient was made aware of positive results of tests.
- Don't file any test result that the physician has not seen and initialed.
- Track tests ordered, receipt of results, and communication to patients.
- Medical Record contents and the order of documents should be consistent.
- Clinical records should be concise.
- Continuity of Care.
- Caregivers are **not** permitted to "*transport*" patients in their own vehicle, nor may they drive the patient or family member's vehicle to either emergent or non-emergent appointments (Walgreens, MD appt., etc.). In an emergency, 911 should be called.

OFFSHORING
&
SUBCONTRACTING

THE IHCS POSITION

Because of contractual obligations to our health plan, IHCS *and* its Network of downstream providers must have programs that reflect compliance with state, federal, health plan and Medicare Chapter 21 guidelines. IHCS uses multiple effective ways of communicating information throughout our Network to remind our agency partners of their many compliance obligations.

These updates are designed to make sure *you* know the system in place to receive, record, respond to and track compliance questions or reports of suspected or detected non-compliance in the areas of real or potential FWA, Complaints to Medicare, Incident Reporting, HIPAA Breaches, etc.

It also is intended for you to be aware that IHCS enforces a no-tolerance policy for retaliation or retribution against any individual who in good faith reports suspected non-compliance.

Providers are hereby reminded that they are protected from retaliation for False Claims Act complaints, as well as any other anti-retaliation protections.

Facts about Offshoring

Offshoring Attestation

What is Offshoring?

Business Owners like YOU and IHCS are the "First line of Defense" in the offshoring process and are required to understand the steps and expectations for offshore operations. Engaging in offshoring activities can pose a significant compliance risk to IHCS business. In **offshore** arrangements, a health care organization's electronic information, which may include confidential business information as well as protected health information (PHI) or other personal information, is either maintained *outside the United State*s or made accessible to persons located outside the United States.

What is Subcontracting?

Any engagement by a network Vendor of a third-party subcontractor (a "Sub-Delegate") to perform any delegated services outlined in their Provider Agreement with IHCS shall be deemed a **sub-contractor** of such services. A Vendor may not **subcontract** its responsibilities as defined in the Provider Agreement without the prior written approval of **IHCS**, which shall be at IHCS's sole discretion.

A network Vendor's role and responsibility requires notifying IHCS at the time they are considering offshoring or subcontracting any activities, domestic or foreign, supporting IHCS business.

Vendors are required to complete an **IHCS Offshore/Subcontracting Attestation Form** annually specific to the line of business their offshore vendor will be supporting. Contact a Provider Relations Team Member today for any additional information on this responsibility.

POLICY:

The Company (IHCS) is committed to establishing protocols for oversight of Offshoring or Subcontracting monitoring in the event it is required.

Integrated Home Care Services, Inc. does not Offshore or Sub-delegate any of its health plan contracted delegated services. However, should the need occur, this policy will address the compliance measures that would be required.

Additionally, should a network downstream provider wish to engage in Offshoring, these enumerated protocols would pertain to them as well as part of the IHCS vendor compliance monitoring program.

PURPOSE:

There are no Federal regulations that prohibit the offshore outsourcing of Medicaid administrative functions. CMS requires that Medicare contractors or subcontractors obtain written approval prior to performing system functions[12] offshore.[13]

Although there are no similar r requirements from CMS for Medicaid, CMS has issued guidance in accordance with the Affordable Care Act (ACA) stating that Medicaid agencies are permitted to provide payments to contractors operating offshore for tasks, including administrative functions that support the administration of the Medicaid program.

The purpose of this policy is to establish a general framework for assessing and ranking all issues of risk involved transparency to our Health Plan partners. This policy is also to establish clearly defined risk metrics, inherent or residual. Aggregated data results will be periodically reported via P.I. and Compliance committee reports to the Executive Committee.

GENERAL PROCEDURES

FOR IHCS:

1. IHCS shall not sub-delegate or offshore any delegated function without health plan's prior written consent. IHCS shall be fully responsible for all enumerated services delegated to Provider via its health plan contract.

2. IHCS acknowledges and agrees that any sub-delegation or offshoring of the delegated functions does not constitute a waiver of Provider's responsibilities under its Health Plan Agreement.

3. IHCS shall ensure complete compliance with all terms and conditions as set forth in its contract.

4. IHCS is responsible for internal oversight in accordance with the current NCQA, AAAHC, CMS or Health Plan standards for delegation oversight.

5. IHCS shall notify Health Plan in writing, within fifteen (15) calendar days in the event of any future decision to Sub-Delegate or Offshore.

6. IHCS shall conduct an annual oversight audit, if required, of any sub-delegated or offshoring activities via Attestation requested by any/all health plans.

FOR NETWORK PROVIDERS:

1. A downstream network provider who engages in Subcontracting or Offshoring activity must report it to IHCS *prior to commencement.*

2. Each provider will be asked to complete an Attestation and indicate what activities have been selected and present this signed Attestation at least *15 calendar days prior to instigation*.

3. The provider will comply with all internal oversight as described in bullets three (3) and four (4) as shown above.

4. The provider will be asked to sign an **Annual Attestation** of any/all subcontracted or offshoring activities by designated Provider Relations personnel. Attestations are required for offshore entities that receive, process, transfer, handle, store, or access PHI in oral, written, or electronic form.

5. Any/All Providers engaging in Offshoring/Subcontracting activities, domestic or foreign, will be reported to Account Management for presentation to the appropriate health plan(s) for transparency and contractual compliance. The IHCS IT department will also be copied on this list.

6. The IHCS Director of Provider Relations in conjunction with the IHCS Compliance Officer may request additional information on any network provider who engages in subcontracting or offshoring activities.

Attestations are required for offshore entities that receive, process, transfer, handle, store, or access PHI in oral, written, or electronic form.

Please notify the Provider Relations Department and complete the Offshoring Attestation Form embedded below.

Offshoring Attestation

IHCS Contact Information

Provider Relations:

Email: providerservices@ihcscorp.com

Phone: (844) 215-4264 ext. 7546

Compliance:

Email: compliance@ihcscorp.com

Phone: (954) 381-7954

IHCS Compliance Resources

IHCS Resource Center

https://ihcscorp.com/resource-center/

FDR Compliance Program Guide

2025 IHCS FDR Compliance Guide

Fraud, Waste, and Abuse Reporting

FWA Reporting Methods

Immediately following this presentation, you will receive a ***Provider Orientation Attestation and Offshoring Attestation.***

Please complete and return as soon as possible.

If you have any questions, please do not hesitate to contact us at Providerservices@ihcscorp.com.