OUR Values

OVERVIEW OF OUR CORPORATE COMPLIANCE PROGRAM, INCLUDING *OUR VALUES*

Ways to report a concern include these:

Compliance website — www.WebReportingHotline.com
Compliance hotline — 888-263-2077

TABLE OF CONTENTS

PRESIDENT'S MESSAGE

Dear Employee:

Corporate policies. Desk procedures. Rules and regulations. There are lots of things that help guide the work we do while we're employed here at BlueCross BlueShield of South Carolina. While these things are important, there is another extremely crucial code of conduct by which we all must live — *Our Values*, or our corporate compliance program. *Our Values* are what we believe in and what we stand for if we want to succeed as individuals — and as a company.

This is your personal copy of *Our Values*, which explains the values of your company — BlueCross BlueShield of South Carolina. These values are shared by our subsidiaries and apply to all of us.

Values are more than fancy sayings we put on pretty posters, and determining *Our Values* was not a task we took lightly. A corporate task force worked very hard to develop them, asking employees at all levels to share their opinions. Then our senior management and our board of directors carefully reviewed the values to make sure we hold ourselves to high standards. When all was said and done, we had developed a corporate compliance program.

Compliance is making sure we obey all rules and laws that concern our type of business. It's a commitment to honest values for our employees and our company. Our program serves several purposes:

- To put *Our Values* in writing so everyone can understand the foundation of our company
- To explain your role in making sure we follow all laws, regulations and policies that concern our business practices
- To explain our management's commitment to following all laws, regulations, standards of care and ethical business practices
- To outline expectations for understanding and following basic legal principles and rules of behavior

Please read this booklet carefully and apply these values to your daily work. Just as you follow desk procedures, so should you follow the path that *Our Values* has set for each of us.

Best regards,

Mike Mizuer, President and CEO

THIS IS NOT A CONTRACT OF EMPLOYMENT. IF YOU ARE AN EMPLOYEE OF BLUE CROSS AND BLUE SHIELD OF SOUTH CAROLINA AND/OR ANY OF ITS SUBSIDIARIES OR AFFILIATES, YOUR EMPLOYMENT REMAINS AT-WILL AND MAY BE TERMINATED BY EITHER PARTY AT ANY TIME, WITH OR WITHOUT NOTICE OR REASON.

DIVERSITY STATEMENT

At BlueCross BlueShield of South Carolina and its subsidiary companies, diversity refers to the collective mixture of differences and similarities. We understand diversity extends beyond race and sex and includes diversity of thought, values, perspectives, approach, expectations and needs. Our ability to meet the expectations of our stakeholders hinges on being a high-performance organization capable of solving problems better and faster than the competition, providing a broad range of products and services, and delivering exemplary customer service — all benefits of a diversified and inclusive workplace.

We realize that diversity impacts every area of our business: health outcomes, business development and retention, employee recruitment and development, our corporate giving efforts, and our workplace culture. For BlueCross BlueShield of South Carolina, diversity matters!

OUR CORPORATE COMPLIANCE PROGRAM

Introduction to *Our Values*

As you know, the corporate compliance program and our code of conduct, *Our Values*, guide all of us to do the right thing. We are committed to conducting business the right way. *Our Values* are what we believe in and what we stand for. Our effective compliance program helps make us successful in gaining new business and retaining our current government and private business contracts.

Our corporate culture is based upon several key values (*Our Values*) that determine how we as individuals and as a corporation function in all facets of our operations. These values must be foremost in our thoughts and actions, and we must assure that these values are observed throughout our company. Failure to comply with the standards of *Our Values* may result in disciplinary action up to and including termination of employment or other relationships for a first offense.

Our corporate compliance program also has oversight of our compliance with federal and state requirements, such as those related to privacy (e.g., HIPAA/HITECH); fraud, waste and abuse (e.g., False Claims Act, Anti-Kickback, etc.); and many others. This refresher training will help guide you through these topics and give you the tools to recognize and report any concerns you have.

What you may not realize is that our Compliance departments, corporate and Celerian Group, have your best interests in mind — we've "got your back." We want to help make things right before they go beyond our control. We need the help of every employee to stay on course and succeed as individuals and a company. It is never a bad idea to contact your Compliance department to ask a question or report a concern.

What Does Our Corporate Compliance Program Do?

- Oversees the entire compliance program, including all of BlueCross' wholly owned subsidiaries
- Ensures issues identified by direct contacts to the Compliance department, to the compliance website or to the Corporate Compliance Hotline are reviewed and/or investigated and that any corrective actions needed are implemented
- Develops ongoing training programs to instruct employees in ethical decision-making
- Helps ensure employees follow all laws that concern our business, perform activities in an ethical manner, avoid conflicts of interest, and maintain proper stewardship of property, customer information and confidential information

OUR VALUES

As previously mentioned, *Our Values* is our code of conduct. It is what we believe in and what we stand for; it guides us to do the right thing. It also helps us to achieve our mission. Our mission is to create value for our members, customers, employees and communities through maintaining a fiscally strong, high-quality organization. This is accomplished through excellence in service; offering efficient and affordable insurance plans and administrative services products; by being the nation's preeminent supplier of high-quality, efficient services for federal and state health care programs; and by using our expertise in information technology and financial services to support and acquire other profitable businesses.

Everyone acting on behalf of the company — employees, managers, officers, board members, contractors, consultants, etc. — is expected to follow the company's code of conduct, *Our Values*, company policies and procedures, and all laws and regulations.

So, what will we use to guide us on this journey? Here are the seven foundations for *Our Values*:

COMMUNICATION

We will support open communication among all employees, customers and other people who work with us. By learning how to talk to each other, we will improve our jobs, the company and ourselves.

- We will talk to our supervisors about our job suggestions, concerns or problems.
- We will treat our coworkers and customers with respect. We will try to understand their points of view by learning about their responsibilities and challenges.
- We will participate in regular staff meetings, peer groups and company surveys when requested by management.
- We will work hard to improve our communications skills and use them effectively.

RESPONSIBILITY

We will understand and take responsibility for our actions. What we do affects the company and those whose personal information we can access.

- We will not reveal or access sensitive information unless specifically authorized and required as part of our job function. This includes:
  - Product information.
  - Our business strategies.
  - Sales information.
  - Marketing plans.
  - Our systems.
  - Finances.
  - Proposal information.
  - Electronic claims, claims histories, enrollment, referrals, authorizations and other claims-related information.
  - PII/PHI.
  - Rate adjustments.
  - Pricing information.
  - Underwriting procedures.
  - Account numbers and passwords.
  - Information about our business partners.
- We will protect and preserve things that belong to the company, including our office equipment and supplies.
- We will guard our customer and billing lists from any outside individual or organization.

- We will use the company's money, assets and proprietary information for appropriate company purposes. We will not use them for others outside the company or ourselves for personal use.
- We will not create or keep any unrecorded funds or assets.
- We will not intentionally make false entries in our company's financial books, reports or other records.
- We will keep employee information confidential.
- We will not process our own, a relative's or a friend's claim or access any related medical information or PHI.
- We will immediately report any suspected or known violations of company policy and/or the *Our Values* code of conduct.
- We will immediately let management know of any problems that arise that affect our performance. Our goal is to ensure that problems are identified and corrected and appropriate individuals are notified.

INTEGRITY

We will meet all our responsibilities in an honest and ethical manner. We will follow all laws, rules and regulations. And remember, just because it may be legal, that doesn't mean it's right. We will maintain the highest ethical and moral standards and look beyond the legal issues.

- We will follow all laws and regulations that apply to our business. We are dedicated to doing the right thing.
- We will not knowingly go after business opportunities that call for us to do anything unethical or illegal.
- We will contact management when we have reason to believe someone has engaged or is engaged in unlawful or unethical acts at work. We will follow the usual chain of management to address our concerns.
- We will ask our management or the corporate compliance officer if we have any questions or concerns about laws, regulations or legal issues.
- We will use honest advertising in our marketing efforts.
- We will pursue our sales goals with the highest ethical standards in mind.
- We will respond honestly and completely when questioned about any work-related activity or any activity outside the company that could create a potential conflict of interest.
- We will not tolerate any false or dishonest billing practices. We will report problems to management immediately for investigation and correction.
- We will not accept kickbacks, bribes or other benefits in exchange for payments, referrals for services or other actions.
- We will not knowingly submit or prepare incorrect, incomplete, false or misleading information or reports.
- We will not provide materially false statements or omit information in connection with any audit or review of financial statements and will not coerce, mislead or fraudulently influence auditors that could result in financial statements being materially misleading.

SERVICE

We will focus on the customer. We must work together to give excellent service and customer satisfaction.

- We will understand what our customers need and expect from us, and we will deliver those products and services to the best of our ability.
- We will treat all our customers with dignity, concern and respect for their well-being.
- We will use sound judgment in giving services to our customers.
- We will respect and assist each other in the performance of our duties. By working together, we can serve our customers better.
- We will give our customers appropriate services that follow all related laws and regulations.
- We will respect the confidential nature of our customers' and business partners' health information.
- We will protect health information from those who do not have the authority to see it or hear about it.
- We will guard the personal privacy of all customers and business partners. We realize our customers trust us not to share information about their medical treatments, health conditions or finances.

PEOPLE

We are committed to the continuing education, well-being and personal growth of all employees.

- We will treat our coworkers with consideration and respect.
- We will make sure job and promotion opportunities are truly equal for all employees. This will be regardless of race, color, national origin, religion, veteran status, disability, gender, age, creed or sexual orientation.
- We will not allow harassment or retaliation in any form.
- We will be sensitive and open to others. We will listen carefully and patiently to suggestions, ideas and concerns.
- We will be open and honest when dealing with our coworkers, management, customers and business partners.
- We will emphasize health, safety and privacy in our workplace.
- We will maintain a drug-free and smoke-free work environment.
- We will respect our coworkers' privacy. We will not talk about health or other private information.
- We will encourage continued education and training so employees can be active partners in our success and growth.

INNOVATION

We will support creativity and innovation. We are willing to take risks in developing and launching new ideas.

- We will share and express our ideas with others, including coworkers, management, the Human Resources department and/or through work enrichment programs that may be available in our divisions.
- We will listen carefully to the ideas of our coworkers. We will use those that will help us in our work.
- We will strive to move forward in our thinking and encourage positive changes to our business.
- We will apply new techniques and technology to help us improve our business.
- We will continue to seek opportunities to improve our jobs and procedures.

QUALITY

We will work to understand and exceed our customers' expectations. Our goal is to do the right thing the first time in a workplace that is supportive, reliable and cost-effective.

- We will strive for excellence in everything we do for our customers, members and ourselves.
- We will perform our jobs to the best of our ability at every level of our organization.
- We will not ignore deficiencies or errors. If we find them, we will bring them to the attention of management.
- We will demonstrate honesty, integrity and fairness in the performance of our duties.
- We will encourage and expect our business partners to have an effective compliance program.

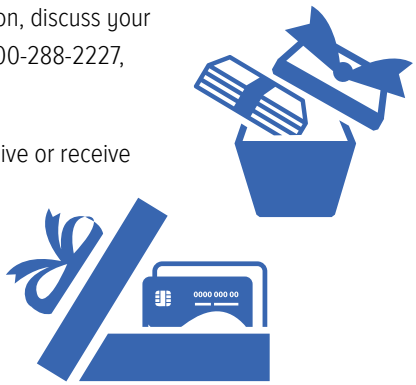
Selected Corporate Policies That Relate to *Our Values*

Conflicts of Interest (Policies 65002, 65205 and 65222)

We will avoid any situation in which a conflict of interest could exist or appear to exist between our personal interests and the business interests of the company. BlueCross encourages all employees to support their communities. Employees should avoid outside jobs or activities that conflict with the employee's current BlueCross position or reflect poorly on the company. Yearly, you (along with all employees, officers and board members) are required to complete a conflict of interest (COI) form that will disclose to the company various types of information about you and your contacts. If any information you provide on this form changes during the year, it is your responsibility to immediately notify your management and fill out a new COI form by selecting the Compliance worklet in OurHRConnect within 30 days of the change.

Gifts and Social Functions, Etc. (Policy 65002)

If, after reviewing the guidelines, you are unsure about accepting or giving a gift or attending a function, discuss your situation with the appropriate management in your area or call the corporate compliance officer at 800-288-2227, ext. 43435. You can also contact your company's compliance department.



This policy applies to all gifts and social/professional functions associated with your work. Gifts you give or receive or functions you attend on a personal basis are not subject to this policy. For example, it is not a conflict of interest if you buy a gift for someone with your own money and give it to them for personal, nonbusiness reasons, even though you may have work associations with the recipient.

Gifts You CAN Accept

A gift with a value of $100 (see **Celerian Group** exception below) or less does not represent a conflict of interest, and you can accept it. Gifts under $100 in value do not have to be reported on the annual conflict of interest form. Some examples of such gifts are logo items from other companies, like umbrellas, keychains or tote bags. Certificates, plaques and other award-type items are also acceptable. Flowers, candy and other food items are acceptable, as well.

Keep in mind that some area management may implement a stricter policy about accepting gifts. It is the responsibility of management to inform you if your area's guidelines are stricter than the above policy.

If you receive a gift valued at more than $100, get approval from your area management before you accept it and be sure to report it on your annual conflict of interest form. In addition, if you receive multiple gifts from the same source and the value of the gifts adds up to more than $100 over the course of a year, you must report all gifts on your conflict of interest form. Also, you must get approval from your management before accepting the gift that puts the annual value of all gifts at more than $100.

EXCEPTION: Celerian Group companies (Palmetto GBA, CDS, CGS, PGBA, JBS, Karna, InStil Health and Medicaid division) employees, contractors and consultants who support government contract work have a $50 gift limit and CANNOT accept ANYTHING of value from anyone or any entity (i.e., doctors, hospitals, vendors, suppliers, beneficiaries, home health agencies, hospices, etc.) that bills or receives funds from a state or federal agency program (e.g., Medicaid, Medicare, Veterans Administration, Tricare, World Trade Center, South Carolina Department of Health and Environmental Control, South Carolina Department of Employment and Workforce, etc.). (See also Policy 65284.)

Any gift or cash award you receive from BlueCross or one of its subsidiaries is acceptable because it never represents a conflict of interest.

Gifts You CANNOT Accept

You can never accept cash or a cash equivalent gift of any amount. You cannot accept ANY gift from a contractor, vendor, or other entity or person if you are in a position to award or give business to such person or entity. Keep in mind, if acceptance of a gift just doesn't feel right, then chances are it isn't right and should not be accepted. If you are not comfortable with receiving a gift, don't accept it.

Gifts You CAN Give

Company logo items of minimal value are acceptable gifts for outside contacts. Certificates of appreciation or recognition are also appropriate gifts you can give. Refreshments provided at meetings or light lunches served to a meeting group are also acceptable.

Gifts You CANNOT Give

Cash gifts are always inappropriate and cannot be offered to anyone. Gifts to others exceeding $100 in value must receive prior approval from your area management. Never offer gifts or refreshments other than the ones outlined in this policy to federal or state employees.

Social/Professional Functions (Policy 65002)

Some of us are invited to attend social functions due to our professional duties with the company. In most cases, the cost of your attendance at such functions is borne by the organization or business sponsoring the event. If the cost of your attendance at a social/professional function exceeds $100, prior approval of your area management is required.

Functions valued at more than $100, such as high-priced restaurant meals, expensive travel or high-cost event tickets, could present the appearance of a conflict of interest when the cost of your attendance is paid by an outside source. So be sure to check with your management before attending.

Political Activity and Contributions (Policy 65002)

- We will not receive any company reimbursement for our political contributions.
- We will follow the laws that limit the use of corporate funds in conjunction with state and federal elections.
- We will not involve the company in any political activity without contacting the Corporate Legal department.

Telephone and Workstation Monitoring (Policy 65205)

All company telephones and workstations are subject to being recorded or monitored by area management or by Corporate Compliance at any time. This is done to ensure quality customer service, compliance with relevant laws and company policies, and for other business and employment reasons. For more information, see Corporate Policy 65205 — Personal Conduct.

Reporting Violations (Policy 65205)

All BlueCross Entity personnel should report known or suspected violations of these policies to their supervisors, their company's compliance officer, a senior BlueCross Entity officer, the Corporate Audit and Compliance division, or a member of the BlueCross Entity Board's Audit and Compliance Committee. All possible measures shall be taken to protect the anonymity and confidentiality of the reporting individual where warranted. Reports may be made anonymously by calling the Corporate Compliance Hotline at 888-263-2077, visiting online at www.WebReportingHotline.com or following the link on My e-Work.

WHAT TO DO IF YOU HAVE A CONCERN

Your Responsibility To Follow *Our Values*

As an employee of BlueCross, you are responsible for knowing what is required under *Our Values* and following these principles. Employees are always expected to be honest, act in good faith and use good judgment. Compliance with these principles is mandatory for every employee. Failure to comply with the standards of *Our Values* will subject you to disciplinary action up to and including termination. If you have questions about these standards or any requirements or responsibilities on your part, you are encouraged to discuss them with your manager, the corporate compliance officer or, if you are a Celerian Group employee, your company's compliance department.

BlueCross expects all employees to show integrity and good judgment when performing duties and representing the company. *Our Values* gives you broad guidelines to follow. Of course, we realize this document does not cover every situation you may come across. For specific company policies and procedures, please refer to this booklet or the Corporate Policies app in OurHRConnect. Your area or division may also have a supplemental policy and procedure manual or code of conduct.

Your Duty To Report

As an employee, you have the right and the responsibility to question or challenge situations in which you suspect that something improper, unethical or illegal is going on. You also have an affirmative duty to report any suspected misconduct or violation of *Our Values* and potential violations of federal, state and local laws and regulations. The company is committed to looking into your concerns and addressing them if they're found to have merit, but we won't know those concerns exist unless you let someone know. Being aware of suspected misconduct and not reporting it may subject you to disciplinary action. If you do report suspected misconduct, you also have a duty to cooperate in investigating the matter.

How To Report a Concern

Once you've decided that you need to talk to someone about your issue or concern, whom should you contact? Fortunately, you have several options:

- Talk to management. We suggest you start with your immediate supervisor. Give your supervisor sufficient time (approximately one week) to resolve the problem. It may be a communication misunderstanding, or management may have a valid reason for a request that you think is a compliance violation. If your supervisor cannot resolve the issue to your satisfaction or you are not comfortable talking to your supervisor, contact your next level of management or another management person in your division.
- Contact the corporate compliance officer, Louis M. McElveen, at 800-288-2227, ext. 43435.
- If you wish to remain **anonymous**, you can also contact our **Corporate Compliance Hotline** at 888-263-2077. This number is not an inside phone number. We have hired an independent company to receive these calls. This company receives all hotline calls at a remote location (through phone lines that are not monitored or owned by the company). If you do not provide your name, the company has no way of obtaining this information — your report can truly be made without the company identifying you. This independent company provides Corporate Compliance with a written summary of your concern or complaint without providing your name unless you provide it to them and give them permission to do so. Corporate Compliance will then investigate the situation. After you call the Corporate Compliance Hotline, you'll receive a callback date and a reference number in case additional information is needed.
- You can also remain anonymous by logging on to My e-Work under the Report Compliance Concerns link, or you can log on from any location to the following website: www.WebReportingHotline.com. This website is anonymous and is hosted by the same independent company that manages our Corporate Compliance Hotline. The same process mentioned above with respect to the Corporate Compliance Hotline applies here. The only difference is that you are choosing to report via the internet as opposed to a telephone call.

- You can also send an anonymous note via interoffice mail to Corporate Compliance Officer (AC-200) or use the drop box if you are employed in Celerian Group.
- In addition, if you work for a **Celerian Group** company, you can contact your company's compliance officer. A list of compliance officers is located on My e-Work under the **Corporate Audit, Compliance, Ethics** link in the Compliance Directory.
- If you need to report suspected fraud, waste or abuse by an employee, provider, member, vendor or other external entity, you can contact the fraud hotline at 800-763-0703.

You can also contact the HR Support Center at 800-288-2227, ext. 46654. Your HR generalist can also be contacted to discuss your issue or concern. As appropriate, Human Resources may refer your issue to other areas (compliance unit or management) or work with other areas to address your concerns. Likewise, if an issue is received through the Corporate Compliance Hotline or directly to one of the compliance units that is an employee relations matter (such as lateness, job selections, dress code, sexual harassment, etc.), these will be referred to Human Resources for appropriate handling.

Investigations

The company will make every attempt to investigate issues reported. Be aware that if you do not provide enough information in your anonymous report, it may limit the company's ability to conduct an investigation and could lead to no corrective action being taken. We must be able to substantiate allegations before taking corrective action. It is for this reason that we encourage you to provide as much information as possible, including your name.

Confidentiality in Reporting

If you choose to include your name when reporting a violation, we will still do our best to maintain your anonymity. For example, sometimes it is impossible to investigate suspected misconduct without identifying the complainant (especially if the matter reported is an employee relations matter). We believe, however, that it is better to come forward than to let the misconduct continue. The company has a nonretaliation policy to protect individuals who report suspected misconduct. Any violations of the nonretaliation policy will result in disciplinary action up to and including termination. We are committed to protecting employees who make good-faith reports of compliance concerns.

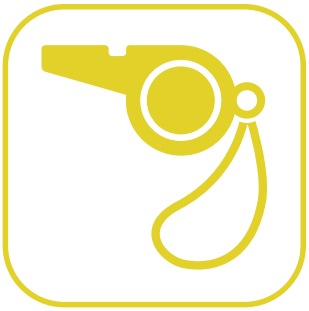
Self-Reporting

Employees will not be exempt from the consequences of their wrongdoing by reporting the wrongdoing. Nor will employees be exempt from the consequences of their inadequate performance by reporting a wrongdoing. However, the consequences from that wrongdoing or inadequate performance may be less severe because the employee has made the self-report. In most cases, an employee's prompt and forthright disclosure of his or her error or wrongdoing will be considered a positive action and consideration will be given to this disclosure.

Nonretaliation

The company's nonretaliation policy (65003 and 65205) is one of the most important elements of our ethics and compliance program. Open communication of issues and concerns by all employees without any fear of retribution or retaliation is vital to the success of the *Our Values* program. We understand that employees may not report concerns for fear of being subjected to retaliation or harassment. However, no supervisor, manager, officer or other employee is permitted to engage in retaliation or any form of harassment directed against an employee who makes a good-faith report of a concern. Keep in mind that acting in bad faith, such as intentionally reporting a false allegation, violates *Our Values* and can subject you to disciplinary action. Any supervisor, manager, officer or other employee who engages in such retribution or harassment is subject to discipline up to and including dismissal for a first offense. However, keep in mind that retaliation does not include appropriate disciplinary action against an employee who may have engaged in wrongdoing or who is not meeting expectations.

Whistleblower Protection



Whistleblower is a common name for someone who reports a wrongdoing to authorities. Several federal laws (e.g., False Claims Act) have adopted that terminology and, more importantly, provided protection for whistleblowers. Federal agencies and their contractors, such as the Celerian Group companies, must protect government contractor employees who act as whistleblowers. Government contractors are prohibited from firing, demoting or otherwise discriminating against an employee in retaliation for that employee disclosing what he or she reasonably believes is:

1. Evidence of gross mismanagement of a government contract.
2. A gross waste of government funds.
3. A substantial and specific danger to public health or safety.
4. An abuse of authority.
5. A substantial violation of law relating to a government contract.

The federal whistleblower laws are very similar to our nonretaliation policy mentioned above. In summary, our employees always have a responsibility to report concerns about potential violations of our corporate values and are not permitted to overlook such violations. The company is firmly committed to a policy that encourages timely disclosure of such concerns and prohibits any retaliation or retribution directed against an employee for making a good-faith report of his or her concern.

Management's Responsibilities

All provisions of the *Our Values* program apply to all BlueCross associates, management, officers and directors. Now that we have informed all associates of the things we expect from everyone under *Our Values*, we want you to know what some of management's special responsibilities are to you under the *Our Values* program.

Management will:

1. Listen to your concerns and questions.
2. Address your concerns or questions by either responding in a timely manner or by routing your concern or issue to the appropriate area for handling and response.
3. Support all compliance efforts in the company and follow the *Our Values* code of conduct.
4. Strive to provide a work environment where employees feel comfortable raising compliance issues or concerns.
5. Encourage compliance initiatives within the work area that promote compliance awareness and reporting.
6. Set the example for all by always conducting themselves in an ethical and honest manner.

Management will not:

1. Ignore reports or questions regarding compliance concerns or issues.
2. Retaliate against or harass in any way any employee or person who raises a compliance issue or concern.
3. Deter an employee from addressing or reporting issues through the company's open-door policy, contacting compliance personnel, the compliance hotline or compliance website, even though it is management's responsibility to get involved at this point.

HIPAA PRIVACY AND SECURITY OVERVIEW

What are the HIPAA Privacy and Security Rules? The Health Insurance Portability and Accountability Act of 1996 (HIPAA) created national standards for protecting the privacy and confidentiality of individuals' medical records and other protected health information (PHI) and the confidentiality, integrity and availability of electronic health information. It also standardized the right to be informed of and control how an individual's health information is used. In addition to HIPAA, Congress passed the HITECH Act in 2009. HITECH, which works in tandem with HIPAA, addresses electronic medical records (ePHI), added privacy and security requirements to certain third parties that we do business with known as business associates, and generally increased the federal government's enforcement powers regarding privacy and security rules. Because these two acts work in tandem, we will refer to them both as "HIPAA" in this manual.

This overview provides the highlights of these regulations. You can find specific policies relating to security and confidentiality of information:

- In corporate policies 65019 and 65206 found in OurHRConnect.
- In the HIPAA Privacy Operational Requirements document located on the Privacy Information page of My e-Work under Privacy and Security.

Training

BlueCross requires that all employees and contractors complete privacy training before they report to their work areas. This will include initial security awareness training. Your department may require additional training related to your job responsibilities.

- The appropriate training department develops this training.
- The privacy office and/or the privacy official for the line of business (LOB) must approve specialized training.
- The department management will ensure departmental HIPAA privacy training is recorded and maintained for a minimum of six years.

If an employee changes jobs within BlueCross or his or her job responsibilities change, current management will evaluate the need for additional training. The Corporate Compliance training department retains HIPAA training records for 10 years.

Our Corporate Privacy and Security Program Structure

Corporate Privacy Officer

The corporate compliance officer, Louis M. McElveen, also serves as the corporate privacy officer. He oversees the development and implementation of corporatewide privacy policies. He coordinates corporate activities with privacy implications. Through his Corporate Privacy office, he also monitors our services and systems to ensure effective privacy practices. The Corporate Privacy office handles complaints and receives requests from individuals related to PHI and other privacy matters. Each LOB also has an assigned privacy official who coordinates with the Corporate Privacy office. You can find a complete list of the company's privacy officials under the Privacy and Security link on My e-Work.

Security Council

The BlueCross Corporate Security Council, chaired by Elizabeth C. Hubbard, is a centralized governing body with the following charter:

To create, review and update the BlueCross BlueShield of South Carolina and any affiliates or subsidiaries it directly or indirectly controls (BlueCross) corporate security policies. The BlueCross corporate security policies define the basic security level of the Information Security Program (ISP) required to be implemented at all BlueCross Business Units (BUs).

The Corporate Security Council also assists with making informed decisions regarding the management of the corporate security policies the Council will additionally serve as the central coordination point for sharing ideas and concerns related to organizational cyber security risk and corporate security policy compliance by each of the BlueCross BUs.

In addition to other topics, the corporate security policies address the subject of electronic protected health information (ePHI) and other sensitive information to ensure BlueCross complies with a basic level of security. As part of this, the Security Council publishes a monthly security bulletin that is distributed via corporatewide email. These security bulletins are quick reads and cover a variety of timely topics to help make us aware of security tools that are available to us or teach us about the various scams that could pose a threat to our company.

HIPAA Privacy

What Is Protected Health Information (PHI)?

PHI is any information in any form or media (electronic, paper or oral) that identifies or could be used to identify an individual that was created or used in the course of providing health care services. It includes billing information and health insurance information. See the definition of PHI in the Glossary in the back of this booklet.

Examples of PHI include:

- Personal information, such as name, address, birth date, phone number or Social Security number.
- Medical information, including health status and medical history.
- Claims-related information.
- Provider/facility information about a member.
- Insurance coverage information.

What Is PII?

Many of our Celerian Group areas also reference the term "personally identifiable information" (PII). While this section mainly addresses PHI, which is included in the HIPAA Privacy Rule, many of these same rules also apply to PII for government contracts. PII includes information that can be used to identify a person, such as the person's name, address, account ID or username. Whereas PHI rules are health-related, PII addresses any information, whether health-related or not. See the definition of PII in the Glossary in the back of this booklet. PII becomes PHI when it is associated with:

- The individual's past, present or future physical or mental health condition.
- The provision of health care to the individual.
- The past, present or future payment for the provision of health care to the individual.

The Centers for Medicare & Medicaid Services (CMS) now considers account IDs and usernames to be PII, and employees should protect this information accordingly.

Federal agencies and their contractors must protect PII by complying with applicable federal statutes, regulations, instructions and memoranda.

Federal contractors are required to limit the collection, use and disclosure of PII to only the minimum necessary to accomplish the intended purpose. This includes but is not limited to an individual's:

- Education.
- Financial transactions.
- Medical, criminal or employment history.
- Distinguishable individual information, such as name, Social Security number, Medicare Beneficiary Identifier, date/place of birth, mother's maiden name and biometric records.
- Any other personal information that is linked or linkable to an individual.

By protecting the PII we handle every day, we protect BlueCross' reputation and earn and retain our customers' trust. While it is important that we do our best to avoid disclosures, it is equally important that we immediately report them if they occur. Hiding a disclosure only makes the problem worse and expands the legal risk for you and the company.

If, in your job function, you are required to make determinations about an individual based on PII, ensure the accuracy, relevance, timeliness and completeness of PII, as is reasonably necessary, to assure fairness in making those determinations. Only use PII for the purposes for which it was collected.

In addition, the Alcohol, Drug Abuse and Mental Health Administration Reorganization Act (ADAMHA) places specific requirements on federal agencies (and their contractors or subcontractors) for the confidentiality and disclosure of records of the identity, prognosis or treatment of any member in connection with a substance abuse, alcoholism or alcohol abuse program.

There are also other federal laws that strictly prohibit the release of alcohol or substance abuse treatment records without the patient's explicit authorization.

When Is Disclosure of PHI Permitted?

An individual's PHI can be disclosed without the individual's authorization for purposes related to the individual's treatment, payment functions or health care operations (TPO) as defined under HIPAA. For example, a health insurer and a patient's provider (e.g., physician) are allowed to discuss details of a patient's claim in the normal course of business. See the definition of TPO in the Glossary in the back of this booklet. In addition, an individual may authorize disclosure of his or her PHI. HIPAA requires an authorization for uses and disclosures of PHI for purposes other than TPO. An authorization is a detailed document that gives BlueCross permission to use PHI for specified purposes, which are generally other than TPO, or to disclose PHI to a third party specified by the individual. When disclosing an individual's PHI to someone other than the individual, you must follow your area's specific procedures. If you receive a request to release or share PHI and you are unsure what to do, contact your management or area privacy official.

Reportable Events

Any time you learn that a person's PHI was sent to the wrong person or company, even if the disclosure was accidental, you must report this immediately to your management. Management must report disclosures to its LOB privacy official and/or compliance unit, in accordance with your company's established procedures. The LOB privacy official must report it to the Corporate Privacy office. If an area does not have a privacy official, management should immediately report the disclosure to the Corporate Privacy office. We are under strict time constraints to report privacy disclosures to certain entities. In some cases, we must report in as little as one hour. Celerian Group may have additional processes, and their employees should also contact their company privacy officer.

Here are some examples of reportable disclosures:

- Sending an email containing PHI to the wrong person
- Misdirecting or sending any information, including correspondence that contains PHI, to the wrong provider, group or individual
- Losing a laptop computer, mobile phone or paper/electronic documents that contain PHI

All personnel should proactively monitor and report any suspected information security incidents and vulnerabilities, not only within their own organization but also associated with external business partners and vendors. These can include but are not limited to:

- Potential malicious activities such as virus infections, server intrusions and network breaches.
- Blackmail.
- Social engineering.
- Information leakage.
- Insider abuse.
- Website defacement.
- Misuse of services, systems or information.
- Violation of computer security policies or procedures.
- Unauthorized computer or data access.

You should immediately report known or suspected security violations to your management and the Technology Support Center (TSC) at extension 42352 (800-288-2227, ext. 42352) or 877-363-8896. To make an anonymous report, visit www.WebReportingHotline.com or select the Report Compliance Concerns link on the My e-Work homepage.

HIPAA Privacy Rights — What Are They?

The HIPAA Privacy Rule ensures certain rights to a member, including:

- The right to receive a Notice of Privacy Practices from his or her health plan and health care provider.
- The right to receive an accounting of disclosures made for purposes other than TPO.
- The right of access to inspect and get a copy of his or her own PHI in the form and format requested (e.g., paper, email, etc.). A response to these requests must be made within 30 days.
- The right to request an amendment to PHI that is incorrect or incomplete.
- The right to request restrictions on uses and disclosures of PHI.
- The right to request that his or her PHI be communicated either by other means or to another location if failure to provide confidential communications could endanger the individual.

HIPAA Security — Preventing HIPAA Disclosures

Confidential or Sensitive Information

It is important to treat all information related to our business as confidential or sensitive whether or not it is PHI. Please make sure that you do not:

- Copy or duplicate information and data, whether confidential/sensitive in nature or not, unless required in support of a business-related responsibility or function.
- Knowingly or willingly conceal, remove, falsify or destroy information in an improper/unapproved manner.
- Use company or customer information for nonbusiness or personal purposes.

Minimum Necessary

You should have access to and use only the minimum amount of PHI necessary to complete your job tasks. You should disclose only the minimum information necessary to accomplish the task. Therefore, before disclosure, you must know the reason for the request or the intended use of the information. In addition, do not store sensitive information on network drives or other electronic storage locations where unauthorized individuals could gain access. Likewise, keep sensitive physical documents in a secure location.

Paper Documents/Forms

- Store documents containing PHI securely to prevent unauthorized viewing when not in use.
- When mailing, ensure PHI is not printed on the outside and the contents cannot be easily seen.
- Whenever possible, mark documents containing PHI to alert readers to the sensitive nature of this information.
- Whenever appropriate, mark documents containing confidential/sensitive information “FOR OFFICIAL USE ONLY” to alert readers to the confidential/sensitive nature of this information.
- Destroy documents containing PHI in a method approved by the organization and/or department, such as approved recycling/shred bins.
- Follow your area’s specific procedures for marking documents according to the data classification.

Voicemail

Because we take an individual's privacy very seriously, it is important NOT to leave any identifiable treatment information on a member's voicemail. An example of this is identifying the code or name of a specific diagnosis. Another example is naming the type of treatment, such as mental health or substance abuse treatment, chemotherapy, or AIDS therapy.

Electronic Data

The HIPAA security regulations protect PHI that is in electronic form (i.e., data on computer drives, tapes, CD-ROMS, etc.). Your departmental HIPAA training will cover data security, but because of its importance to our organization, here are some security highlights:

Workstation and PHI Security

ALWAYS

- Lock or secure terminals when leaving them unattended to prevent others from accessing data through your workstation. You can secure your computer by pressing Ctrl, Alt, Delete and then selecting Lock Workstation or pressing the Windows key and L.
- Close out your applications, select the button at the lower left-hand side of the screen and select Restart from the menu when you are ready to leave work for the day. This allows installed software updates to take effect.
- Follow your area's procedures for working remotely, training room workstations and other unique arrangements. Otherwise, leave the workstation at the Windows login screen.
- Protect mobile computer devices (laptops, electronic notebooks, etc.) just as you would a desktop computer, with additional physical protection in place at all times to safeguard both confidential/sensitive information and to protect against theft or loss.
- Secure laptops with approved security cables while at work. If you take a computer out of the office, protect the computer with a locking cable or secure it out of sight.

- Immediately report all lost or stolen equipment, known or suspected security incidents, known or suspected information security policy violations or compromises, or suspicious activity to the TSC and your compliance office. Known or suspected security incidents are inclusive of an actual or potential loss of control or compromise, whether intentional or unintentional, of authenticator, password or sensitive information (including PII).

NEVER

- Move any computer equipment or plug computer cables into the walls without proper authorization. This is the responsibility of Desktop Support or the IT organization responsible for workstation support.
- Install or use an unapproved desktop modem or analog line.
- Store PHI on local drives or removable media, unless there is a specific business need to do so and it is done using authorized encryption methods and stored into an encrypted container, when needed. Information of this type is best stored on the network in a secure location.
- Allow an unauthorized person to view PHI on your computer monitor or work area. If you work with PHI, consider using a privacy screen or repositioning your monitor for privacy.
- Install personal software on company workstations or use company workstations for personal use.
- Store any PHI or other confidential/sensitive information on a laptop or work-at-home computer without prior management approval.
- Use personally owned computers or portable devices, such as laptops or noncompany devices (USB drives), to access, store or process business-related PHI or other confidential/sensitive information without authorization and appropriate safeguards.
- Direct, encourage or allow others to use another person's account, identity or password.
- Permit unauthorized users to use company equipment and/or software.

As our business requires more interaction with hosted and cloud-based systems, individuals must be mindful of any posted/uploaded content. This applies to business-specific applications like OurHRConnect or the Learning Management System and social media platforms like Facebook and Instagram. All individuals MUST review materials, documents, photos and any other content to ensure it does NOT include PHI/PII. Any PHI/PII content uploaded to these applications/sites may lead to disciplinary action up to and including termination.

Storage of PHI on Removable Media

Removable media devices, such as USB portable flash memory devices (jump drives) and optical discs (BD-ROM, DVD-ROM, CD-ROM, etc.), must be corporate-owned devices and use corporate-approved encryption methods appropriate for your line of business. The use of removable media requires prior approval by your vice president. Responsible management must authorize the removal of media containing PHI and PII from the work area. Features allowing the transfer of data to these devices have been disabled by default. The use of corporate-owned portable storage devices on external information systems (systems residing on any network outside of BlueCross) is prohibited.

Remote Access — Wireless

Employees are not allowed to connect wireless routers and other wireless access points (WAP) to BlueCross equipment or property without proper authorization.

Unauthorized operation of personal wireless access points while on BlueCross premises or connection to a public or private wireless network while also connected to the BlueCross network is not allowed.

Mobile Phones

Employees must adhere to company policy on cellphone and mobile device usage.

- Users connecting to the BlueCross email system via a device with a mobile operating system will use LOB-approved methods to view emails or download attachments that contain sensitive information.
- If sensitive information is viewed on the mobile operating system device, the user must enable a password or an authenticated screen lock, which is available on the device.
- If sensitive information has been stored on the device, the data must be deleted when it is no longer needed.
- Sensitive information must not be sent via text message or non-company-owned instant messaging applications.
- If a mobile operating system device that has been used for email access is lost, the user must:
  - Change his or her BlueCross email password to protect the account from incidental access.
  - Alert his or her manager and the Technology Support Center (TSC) that the device was lost/stolen, provide the TSC with the method of accessing email and tell the TSC if any abnormal activity has been observed.

Sending Emails

Any sensitive information that must be transmitted over the internet, such as emails, must be encrypted using an approved and authorized encryption tool. Most BlueCross employees, with exceptions listed in the following paragraph, can send PHI via Microsoft Outlook to someone outside BlueCross or its subsidiaries by adding [SECURE] at the beginning of the email subject line (include the brackets). Your email (and attachments) will automatically be encrypted. Do not include any identifying information (name, Social Security number, etc.) in the subject line since this line is not encrypted. This will only work when sending an email externally from an internal source. This will not work from an external email address.

Employees of Palmetto GBA, CGS Administrators or Companion Data Services cannot transmit confidential data through the internet unless that data is encrypted in accordance with these companies' specific requirements and specifications.

Some Windows programs, such as Excel, have encryption capability. However, the encryption in these programs is very weak, and it's against corporate policy to rely on them.

Here are some additional thoughts on emails:

- Email messages sent or received via the corporate email system are the property of the organization and can be reviewed at any time by appropriate individuals within the organization.
- A good rule of thumb is to never put in an email message anything you would not want printed in a newspaper.
- The exchange of chain letters, pornographic material or material deemed offensive to others is never allowed. Offenders are subject to disciplinary action. Sending or posting of threatening, harassing, intimidating or abusive material about others in public or private messages or forums is never allowed.
- Do not use your company-provided identifiers (e.g. email address) and authentication secrets (e.g., passwords) to create personal accounts on external websites/applications.
- Do not use a work email address and other information or resources to create personal commercial accounts for the purpose of receiving notifications (e.g., sales discounts, marketing, etc.), setting up a personal business or website, and signing up for personal memberships that are not work-related.

System Password Security

- All passwords shall have a format of sufficient complexity to resist guessing and persistent sophisticated (brute-force) attacks. Passwords should consist of a minimum of eight alphanumeric characters consisting of at least one number, one special character and at least one capital letter. Special characters are limited to @, # or $. In some areas, these requirements can be different. For example, PGBA areas require a minimum of 15 characters for passwords.
- Passwords should not consist of common words found in the dictionary, your names, pets' names, dates of birth or any other identifiable phrases associated with you.
- Never share or store passwords in such a manner as to permit another to gain access to them.
- For Celerian Group, do not use personally owned or noncompany-issued devices to access, process or connect to the company's network or systems. Follow your LOB's rules for the use of noncompany-owned devices.
- Change your password when the system requires it. The Technology Support Center (TSC) will not call or email you requesting a password change.
- Passwords must be changed at least every 30 days, immediately in the event of known or suspected compromise, and immediately upon system installation (e.g., default or vendor-supplied passwords).

Social Media

Social media isn't just Facebook, Twitter or Instagram. It includes all means of communicating or posting information or content of any sort on the internet, including posting anything to your own or someone else's blog, personal website, social networking or affinity website, web bulletin board, or a chat room, whether or not associated or affiliated with the company.

- You should not reveal PHI, PII, trade secrets or information subject to the company's attorney-client privilege nor information related to the company's members, subscribers, vendors or customers.
- You should review items (photos, screenshots, etc.) before you post them on social media, as they may contain PHI, PII, confidential information or proprietary information.
- You should not use social media to contact or communicate with the press or the media on the company's behalf or in a manner that could reasonably be attributed to the company without receiving prior, written authorization from Corporate Marketing Communications.
- You should refrain from using social media while on work time or on equipment the company provides unless it is work-related as your manager authorized or otherwise consistent with company policy. Use of social media network sites is monitored.
- You should refrain from posting inappropriate material that includes discriminatory remarks, harassment, maliciously false information, threats of violence or similar conduct that could reasonably be associated with the company.

Internet Usage

Use of the internet is reserved for authorized business purposes only. Internet usage is subject to being monitored and recorded.

You are prohibited from using company resources for any of these activities:

- Conducting any personal commercial or for-profit activity
- Using peer-to-peer software (i.e., instant-messaging software) without proper authorization
- Operating unapproved websites
- Incurring more than minimal additional expense, such as using nontrivial amounts of storage space or bandwidth for personal files or photos
- Using the internet or workstation to play games, visit chat rooms or gamble

Data downloaded from the internet will be scanned for computer viruses.

Insider Security Threats

To protect confidential and sensitive information from potential external threats like phishing and hacking attempts, we have developed both physical and electronic protections. We have trained employees and contractors to be alert to these dangers from outside our company. There is another, possibly greater threat from employees and contractors who have legitimate access to confidential and sensitive information. Information leakage is a type of insider threat whether it is intentional or unintentional. In this section, we will focus on recognizing possible intentional threats from employees or contractors. It is our responsibility to be alert to and protect our data and equipment from internal threats, but how can we identify them? Here are some potential warning signs that an employee or contractor could be a threat:

- Persons attempting to acquire accesses not needed for their jobs
- Persons bullying or harassing coworkers to give them information
- Persons with unexplained access to financial resources
- Persons displaying workplace violence
- Persons committing other serious violations of company policy, procedure, directives, practices or rules
- Persons who suddenly begin working odd hours without authorization
- Persons who are overly inquisitive of coworkers' financial status
- Persons copying large quantities of information that seem out of the ordinary
- Persons using personal devices, such as smartphones, to take photographs in the work areas
- Persons who have a sudden interest in business strategies or procurement activities outside the realm of their job requirements
- Persons who are examining contents of a coworker's desk and/or office without any business purpose to do so

If you have concerns about behaviors that lead you to believe an insider threat may exist, you should report them to your manager, Compliance, Security or HR. Concerns can also be reported anonymously using the hotline (888-263-2077) or the internet (www.WebReportingHotline.com). Please be sure to include enough information so the issue can be investigated.

External Security Threats

On any given day, you can read about a successful cyberattack on a significant business. Cybercrimes are constantly on the rise and the methods cybercriminals are using are constantly evolving. Our IT security teams continue to provide us with a robust security system to protect our business from these bad actors. However, it is up to all of us, as employees and contractors, to keep up to date with the methods and techniques cybercriminals use and to remain vigilant in our day-to-day routines to avoid falling into their traps. We are the first line of defense. As we look at some of the methods these bad actors use, you will notice emails are a common thread. What follows is a list of various common techniques to be aware of:

Social Engineering

Beware of social engineering scams designed to convince you that you are required to reveal your password or other secure information. While most social engineering is considered to be related to emails, keep in mind that it can come in the form of telephone calls as well. Remember, the TSC should NEVER ask you for your password. Social engineering is a low-tech strategy cyberattackers use that relies heavily on human interaction and often involves tricking people into breaking standard security practices. The success of social engineering techniques depends on attackers' ability to manipulate victims into performing certain actions or providing confidential information. They may attempt to access computer networks or data stores by gaining the confidence of authorized users or stealing those users' credentials to masquerade as trusted insiders. It is common for social engineers to rely on the natural helpfulness of people or to attempt to exploit their perceived personality weaknesses. For example, they may call with a feigned urgent problem that requires immediate network access. Urgency is a common tool they use to convince you to make a quick decision or bypass normal operating procedures. Today, social engineering is recognized as one of the greatest security threats facing organizations. When successful, many social engineering attacks enable attackers to gain access to confidential information. While some of these techniques below may seem complicated or difficult to understand, please keep in mind that, no matter what technique the bad actors use, our job is the same, which is to be ever vigilant with external emails, internet downloads and external phone calls. To assist us with this, our Outlook email system identifies emails received from external sources by inserting [EXTERNAL] in the subject line. Whenever you see this, it is an indicator to be wary of the sender and use cautious judgement.

Here are some specific types of social engineering:

Pretexting is the use of an invented scenario to try to get secure information. A caller or emailer uses known information (birthdate, address, etc.) to add legitimacy to the request for more detailed information or passwords. Pretexting includes some dialogue or back-and-forth (especially over the phone). Pretexting sometimes involves impersonating executives. Think of the people who pretext as modern-day con artists.

Phishing is the use of fraudulent email requesting verification of information or passwords posing as a trustworthy organization. It may contain a warning of a dire consequence if verification is not urgently completed. Many phishing emails take advantage of current events, such as epidemics, holidays and natural disasters. The email usually contains a link to a website that looks legitimate — with company logos and content — and has a form requesting entry of a password or other secure information.

Don't Be Phish Bait

As attackers get smarter, phishing emails become more sophisticated and credible in appearance. It's easy to fabricate an email and give the appearance it came from someone you know. The links may look real yet take you somewhere completely different than expected. The best defense is vigilance. If you don't know the sender or weren't expecting an email from that sender, be suspicious.

- Do NOT open links/attachments.
- Do NOT respond to the email.
- Do NOT forward the email to another user.
- If you feel the email could be valid, contact the sender using information from legitimate sources. Do NOT use information from the email to facilitate contact. If validated, respond as necessary.
- Select the Phish Alert Report button.
- If you opened links/attachments, entered data or responded to a suspicious email, report it using the Phish Alert Report button. If you receive a message that the email was part of a test, no further action is required. If the email was not part of a test, contact the Technology Support Center (TSC) at extension 42352, (800-288-2227, ext. 42352) or 877-363-8896.
- For those external businesses that don't contact the TSC for support, use your company's internal processes. If unsure of who to call, refer to your manager.

For more information, go to the Security Awareness page on My e-Work, where you will find the Security Bulletins page on this subject. See the bulletin from June 2021.

If you accidentally open a link or attachment, keep in mind that it may look just like a familiar site, application or document. Remember that if you enter information, such as your ID and password, you might be giving it to a criminal. Take action as soon as you realize you've been duped. Report it to the TSC and change your password immediately through the correct channels.

Whaling is a specific form of phishing. It targets upper management in private companies. The objective is for upper management to divulge confidential company information. Whaling involves a webpage or an email with a link or attachment that masquerades as legitimate and urgent. The content of a whaling attack is tailored for upper management and usually involves some kind of falsified companywide concern.

Vishing is the fraudulent practice of making phone calls or leaving voice messages purporting to be from reputable companies to induce individuals to reveal personal information, such as bank details and credit card numbers.

Malware is a catch-all term for any type of malicious software designed to harm or exploit any programmable device, service or network. Cybercriminals typically use it to extract data they can leverage over victims for financial gain. That data can range from financial data to health care records to personal emails and passwords — the possibilities of what sort of information can be compromised have become endless. Malware is typically introduced to a computer system through external emails and/or file downloads from external sources, such as the internet. Two of the most common malwares are ransomware and viruses.

Ransomware is a type of malware that prevents or limits users from accessing their computer system, either by locking the system's screen or by locking the users' files unless a ransom is paid. As you may have seen in the news, ransomware attacks have become a more common and lucrative business for bad actors. Whereas many cyberattacks are aimed at stealing confidential information, the goal of ransomware is to shut down a company's computer system until a sum of money is paid to the criminals. These criminals typically require payment in the form of cryptocurrencies, which cannot be traced. We should all be aware that selecting a link from an email, opening an email attachment or downloading a file from the internet could bring ransomware into our system. Our IT Security has state-of-the-art software to thwart these attacks, but the criminals are always evolving, and we can never completely rely on defensive software to do the job. Our vigilance is our greatest defense.

Computer viruses are a type of malware that earned their name because of how they spread by "infecting" other files on a computer or network. A virus can cause damage to programs, data or equipment. Viruses can also interfere with access to network resources, such as file servers, printers and mainframes. An up-to-date antivirus program is used on all company-owned computers. Do not disable or interrupt antivirus scans or other approved security mechanisms and software.

Potential virus warning signs include:

- Warning messages from antivirus software.
- Strange messages or graphics.
- Missing files or data.
- Running out of memory space.
- Programs taking longer than normal to load.

Logon Monitoring

One of our standard but very important security controls relates to logging into the network. As you may know, if you (or an outsider) enter an incorrect password three times in a row, your account will be locked out of the network. If you are locked out of the network, you can call the Technology Support Center at extension 42352 (803-264-2352) for a password reset. Data Security Administration, or any independent entity that performs the data security administration function, will monitor invalid logon and access violation reports and report findings to the appropriate level of management.

Physical Security/Piggybacking

Access to all locations must be controlled. The following points regarding ID badges apply to those locations with a security card access system installed. Federal privacy laws and client contracts require us to secure our buildings and data. This means every person entering a BlueCross facility must have proper permission and obey these rules:

- Employees must wear ID badges in plain view at all times when in a BlueCross building. Wearing badges out of sight in a pocket, purse or briefcase is improper and can result in disciplinary action. You should politely challenge any individual who does not have an approved ID badge displayed. Individuals without badges should be escorted to the nearest security station for assistance.
- If your badge does not allow you access, you should proceed outside the building to the main entrance to the security desk to get appropriate access.
- If you forget or lose your badge, you must enter through the main entrance, attempt to contact a member of your direct management team to sign you in, or go to the security desk and follow established procedures to get a temporary badge. Temporary badges are activated for one day only. At the end of the day, they are disabled. When badges are lost, managers can request a replacement by emailing Security.Tower@bcbssc.com.
- Each employee must use his or her personal badge to enter a facility or restricted area. It is a violation for anyone to use another employee's badge.
- Never allow another individual to enter any secured facility on your ID badge. This is called "piggybacking" and is against BlueCross corporate policy. A piggybacking violation has occurred when:
  - You allow someone to enter behind you without first closing the door and ensuring the person swipes his or her badge.
  - You follow someone in without allowing the door to close and swiping your own badge.
  - You witness someone piggybacking and don't offer to escort him or her to the nearest security station.
  - Your offer to escort to a security station is refused, and you don't report it.

Termination/Transfer of an Employee

- If you are in management, you must complete the termination process in OurHRConnect before or on the effective date of termination of an employee.
- As a manager, you must follow the appropriate procedures to notify data security administrators of any system access changes needed when an employee transfers to or from your department. You are responsible for ensuring your employees have the minimum necessary access to perform their job functions.
- When you end your employment with BlueCross, you must turn in your security badge to your manager, supervisor, Human Resources office or Security and all other I/S-related, company-owned property to your manager.
- Follow any additional termination/transfer procedures required in your area.

An example of a system access change that is often overlooked is a shared faxgate number. In some areas, the faxgate number is shared by multiple users. If one of the users either leaves the company or transfers to another area of the company, the password for the faxgate must be changed.

Penalties for Violations

If you violate our corporate privacy and security rules, you will be subject to disciplinary action up to and including termination. Many of our privacy and security rules are designed around the federal HIPAA rules. HIPAA rules are enforced by the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR). OCR also has the power to impose financial penalties on companies for violations.

Work-From-Home (WFH) Guidelines

NOTE: Associates working for **Celerian Group** often have stricter WFH privacy and security requirements with which they must comply and, therefore, should refer to their WFH resources for guidance. If associates do not know how to locate their WFH guidelines, they can contact their management or their compliance officer.

General Guidelines

WFH guidelines can be found under the COVID-19 and Remote Worker apps in OurHRConnect.

Working from home introduces unique risks that must be addressed to protect the privacy and security of member and company information. Although we commonly use the phrase "work-from-home," these guidelines apply to any work being performed at a remote location. When working remotely, you should ensure distractions are not introduced that may conflict with your productivity and dedication during this time. Be sure you understand all additional expectations set by your managers and follow general best practices expected by your management. When working remotely, it can be easy to feel isolated. Keep your manager, coworkers and clients updated on your schedule, progress and availability.

Workspace Security

Meeting our corporate work-from-home guidelines requires a separate workspace. Your home workspace should be treated as an extension of the workspace in our facilities. You will need to follow the same requirements and restrictions as if you were working on-site. If at any time you or your manager do not believe internal or external requirements are being followed, it may result in the termination of the remote connection and the WFH arrangement.

Here are some workspace security guidelines:

- Familiarize and optimize your at-home network environment. A comfortable chair and table or desk would be ideal.
- Be aware of auto-recording smart devices in the home. Specific smart devices used in homes often have "stored records" picked up by their microphones. Ensure these devices are not in range of any conference calls or sensitive "read-aloud" information. If they are, disabling the device's ability to listen and respond during such activity is recommended.
- If your job entails discussing member information on the phone, have these discussions in a private area.
- Keep in mind you may likely now have sensitive information on the computer screen in your home. Be sure the computer screen is not viewable by anyone who may be in the area in which you are working.
- If your room has a window, be sure the computer screen cannot be seen through the window from the outside.
- Do not allow family members to help do your work.

Computer/Data Security

In some cases, a WFH employee will be issued a company PC for use inside his or her home. With the appropriate approvals, a WFH employee may use a personal PC to connect with the network provided the necessary security protocols (i.e., RSA token or SecureID) are in place. Here are some computer security guidelines:

- HIPAA requirements for PII/PHI and its handling are still in effect for the WFH environment, and the employee is now solely responsible to safeguard the display of sensitive information in his or her home.
- If you're using your own computer or mobile device (something not issued by your organization), make sure you have enabled basic security features. Simply enabling the PIN, fingerprint or facial ID feature will prevent anyone from getting on your device should you walk away from it. Any PIN or password you use should be hard to guess.

- Unauthorized personnel should not access or view sensitive information displayed on the WFH's personal computer and smartphone.
- Lock your computer (activate the screen saver) any time you step away from your work area. Logging off is required when leaving your work area for an extended period of time and at the end of each workday.
- At no time should photos be taken that include the computer screen or the immediate vicinity. Today's cameras are high resolution, and an image taken at a distance may still allow a viewer to clearly read something written down on paper or displayed on a screen. Even inadvertent pictures taken of sensitive information and posted on social media can lead to disciplinary actions up to and including termination.
- When using a camera that is attached to your computer for video conferencing, be sure to disconnect the camera or shutter the camera lens when it is not in use. Cameras for computers should also have an indicator that lets you know when the camera is in use.
- When you finish your work for the day, make sure you log out and, if using a company computer, make sure you restart it. Remember to lock and/or log completely out of your PC during times of non-use.
- If you're seeing unusual or suspicious activity on any device you're using to telework (computer, mobile device or home network) ask for help — better safe than sorry. Contact the TSC at 800-288-2227, ext. 42352, or 877-363-8896.
- Keep your computers and mobile devices patched and updated. Most provide an option to check and install updates automatically. Enabling that option can be a good idea if you don't want to check for updates periodically.
- Limit bandwidth usage by reducing long stretches of open access when performing non-access-related activity (e.g., conference calls). Internet streaming services for television, movies, videos, music, gaming, etc. can negatively affect the performance of your WFH environment, even though those services are not in use on the WFH PC. Limitations may need to be set for usage in the home during your working hours should any of these services negatively afffect your bandwidth.

Document Security

- Papers or files containing PHI should never be left unattended.
- Have a designated room with a door that can be locked to protect any hard copy documents that contain PHI.
- Store all hard copy documents in a desk drawer or filing cabinet.
- Shred or destroy any hard copy documents that are no longer needed. Do not simply throw them in the trash.

Additional Guidelines for Managers of WFH Employees

Managing WFH employees can be challenging. You should be very familiar with the WFH employee guidelines. Another way you can be a more effective manager of WFH employees is to:

- Set clear written expectations for your employees, articulating WFH requirements such as:
  - Required email and phone responses within a departmentally determined time frame.
  - A valid phone number and internet connection with the bandwidth needs of a WFH environment.
  - Documenting the WFH employee's agreed-upon work schedule.
  - Regularly scheduled "check-in" periods.

Changes to Policies and Procedures

BlueCross will amend its policies and procedures as necessary to comply with changes in the privacy and security rules. The Corporate Privacy office, in coordination with the Legal department and the Security Council, will track material changes to laws and regulations. They will recommend changes to corporate policies and procedures as necessary to comply with changes in the law.

How To Respond If You Are Contacted by a Federal or State Agency Representative for Information Regarding Company Business

Given the nature of our business, we routinely deal with various federal and state governments' regulatory and investigative agencies. We can be asked to cooperate with a government investigation or to respond to a request for information regarding company business. The request can come directly to management or you can be contacted individually. If you receive a subpoena, immediately notify your management and the Law department. If a government investigator contacts you at home or at work, here are some things you should know.

The investigator(s) has the right to:

- Contact and request to speak to you.
- Conduct the interview in pairs — one to ask questions and one to take notes.

You have the right to:

- Request identification verification and the reason for the interview.
- Speak with the investigator or decline the interview.
- Request the presence of legal counsel from the corporate Law department.

Whatever you decide about participating in the interview, please notify the Compliance or the Law department if a government investigator contacts you. If you do decide to speak with the investigator, you should always tell the truth! There is no retaliation just for speaking with the investigator.

You cannot provide documents or data that belong to BlueCross, or that are in our custody and control, in response to a government request for information without first notifying management to get authorization from the Compliance department and the Law department.

NOTE: Some employees associated with PGBA and Medicare can be required to submit to a background check by federal investigators. This is not the same as a government agency representative asking for company business information. Also, this section does not apply to routine involvement that some of our Medicare and PGBA areas have with governmental agencies related to fraud, waste and abuse activities within the Medicare and PGBA programs.

FRAUD, WASTE, ABUSE AND RELATED FEDERAL LAWS

The health care industry is under intense scrutiny by federal and state agencies.

Tens of billions of dollars each year are lost to fraud, waste and abuse (FWA). This translates to higher premiums and higher health care costs for all of us.

We have a comprehensive FWA compliance program in place, including policies and procedures to address the prevention of fraud, waste and abuse. We actively pursue all suspected cases of fraud, waste and abuse and work with appropriate government agencies as needed. As you may know, we outsource some processes to third-party vendors. Many of these vendors, especially those that support lines of business that receive government funding, are also required to have FWA compliance programs. As part of our program, our LOBs communicate with those vendors on a regular basis to confirm they have a functioning FWA compliance program in place.

Fraud and abuse are two of the reasons federal and state health care programs are facing financial difficulty, and the public believes something should be done about it. We all have an obligation and responsibility to the company to help prevent and identify fraud and abuse by immediately reporting any suspected or known violations to the corporate compliance office.

Traditionally, we think of fraud and abuse as being committed against the company by outside entities or persons (i.e., fraudulent providers). But fraud does occur within companies, committed by its own employees. Penalties and consequences for fraud and abuse are just as harsh and detrimental to the company and its employees as they are to providers or others when caught.

The effects of fraud and abuse include:

- Increased health care costs due to unrecovered fraudulent expenses.
- Lost business opportunities/contracts leading to a reduction in workforce.
- Increased burdens on federal, state or local tax funds and a reduction in the level of services to members due to increased audit and security levels.
- Entities or individuals who receive funds from BlueCross or a government-sponsored health care program, including providers, members, employees and vendors, being subject to penalties for fraud.

Penalties for fraud include:

- Potential monetary penalties ranging from $13,508 to $27,018 for each false claim and an additional fine of up to three times the total amount of false payments that were made.
- Additional civil and criminal charges.
- Revocation of licenses to do business and exclusion from participation in all federally funded health care programs.

Because of this, it is important you understand the difference between fraud, waste and abuse in addition to the effects, penalties, laws and preventive measures.

Fraud — The intentional misrepresentation or concealment of truth for the purpose of taking, or attempting to take, money, property or other company assets by providers, insureds, agents, group representatives, employees or other individuals. In the health care world, we could say it's when someone intentionally lies to get a health care benefit to themselves or others they are not entitled to. The most common kind of health care fraud involves false statements or deliberate omission of information that is critical in the determination of authorization and payment for services. Health care fraud can result in significant monetary liabilities and, in some cases, subject the perpetrator to criminal prosecution. Some examples of health care fraud include:

- Provider fraud.
  - When a physician intentionally bills for services that were never rendered
  - Intentionally billing for more-expensive services or procedures than were provided or performed, commonly known as "upcoding"
  - Falsifying a patient's diagnosis to justify tests, surgeries or other procedures that aren't medically necessary
  - Prescribing controlled substances with no legitimate medical purpose
  - Accepting kickbacks for patient referrals
- Member fraud.
  - Falsifying information

Waste and abuse are unintentional acts, whereas fraud is intentional. For this training, we have combined waste and abuse because they are similar. **Waste** is the inappropriate use of health care funds or resources without a justifiable need to do so. Waste relates to mismanagement, inappropriate actions and inadequate oversight. **Abuse** is a practice that is inconsistent with sound medical or business practices that may directly or indirectly result in unnecessary costs to a health care program. Abuse can occur when services are used that are excessive or unnecessary, when less-expensive treatment would be as effective, or when billing or charging does not conform to requirements (e.g., a physician orders tests for a patient that are unnecessary based on standard medical procedures).

If you need to report suspected fraud, waste or abuse by an employee, provider, member, vendor or other external entity, you can contact the fraud hotline at 800-763-0703.

Examples of Federal Statutes Related to Fraud, Waste and Abuse

Exclusion Statue — The Office of Inspector General (OIG), which is a branch of HHS, is required by law to exclude any individual who has been convicted of patient abuse, Medicare or Medicaid fraud, and similar unlawful activities from participating in any other federally funded health care program. In other words, exclusion prevents a person (physician) or entity from directly billing Medicare for any items or services. In addition to these mandatory exclusions, OIG has the ability to exclude other individuals based on other health care criteria, such as misdemeanor convictions, physician license suspensions, engaging in illegal kickbacks and others.

False Claims Act — This prohibits knowingly presenting to the federal government a false or fraudulent claim for payment or approval. It prohibits knowingly using a false record or statement to get a false or fraudulent claim paid or approved by the federal government or its agents. It also protects individuals from retaliation for reporting suspected fraud and abuse. Perpetrators could be subject to imprisonment and monetary penalties of up to three times the amount of the fraudulent claims.

Anti-Kickback Statute — This makes it a crime to knowingly and willfully offer, pay, solicit or receive remuneration to induce or reward patient referrals or generate business under the Medicare or other federal health care programs. Example: A provider receives cash or below-fair-market-value rent for medical office space in exchange for referrals. Perpetrators could be subject to imprisonment and monetary penalties.

Physician Self-Referral Law (Stark Law) — This law prohibits a physician from referring patients to receive "designated health services" payable by Medicare or Medicaid to an entity with which the physician or a member of the physician's immediate family has a financial relationship, unless an exception applies. Example: A physician refers a member for a designated health service to a clinic where the physician has an investment interest. Physicians who violate the Stark Law are subject to fines, repayment of claims and potential exclusion from participation in federal health care programs.

The Money Laundering Control Act — This is a United States Act of Congress that makes money laundering a federal crime. It prohibits individuals from engaging in a financial transaction with proceeds that were generated from certain specific crimes, known as "specified unlawful activities."

Glossary

Abuse — Improper and excessive use of benefits or services by providers or members. Abuse can occur when services are used that are excessive or unnecessary, when less-expensive treatment would be as effective, or when billing or charging does not conform to requirements.

Authorization — Permission given by an individual to use or disclose his or her protected health information (PHI) for specified purposes.

Breach — The unauthorized acquisition, access, use or disclosure of PHI that compromises the security or privacy of the information. Breach does not include:

- The unintentional acquisition, access or use of PHI by a workforce member acting under the authority of a covered entity or business associate.
- The inadvertent disclosure of PHI by one person authorized to access PHI to another person authorized to access PHI at the same covered entity or business associate. In either case, the information cannot be further used or disclosed in a manner not permitted by the Privacy Rule.
- Disclosures to an unauthorized person/entity if the covered entity or business associate has a good-faith belief that the unauthorized person/entity would not reasonably have been able to retain the information.

Business Associate (BA) — A person or entity, not a member of the BlueCross workforce, who provides certain functions, activities or services on behalf of BlueCross that involve the use and/or disclosure of PHI. For example, when we outsource a function or process to a third party that includes our customers' PHI, then that vendor would be a BA and subject to the HIPAA Privacy and Security Rules.

CMS — Centers for Medicare & Medicaid Services.

Covered Entity — A health plan, a health care clearinghouse or a health care provider (but only if the provider transmits health information electronically in connection with a standard transaction).

Fraud — The intentional misrepresentation or concealment of truth for the purpose of taking or attempting to take money, property or other company assets by providers, insureds, agents, group representatives, employees or other individuals.

Health Information — Information created or received by a health care provider, health plan, public health authority, employer or clearinghouse that relates to an individual's physical or mental health or condition or provision of, or payment for, that individual's health care.

Individual — A person who is the subject of personally identifiable information and/or protected health information.

Individually Identifiable Health Information (also called personally identifiable information) — Any health information (including demographic data) that permits identification of the individual or that could reasonably be used alone or in combination with other available information to identify the individual.

Information Leakage — Actions of revealing information to an unauthorized party. Human factors cause the issue of information leakage. Human factors can be categorized as intentional actions and unintentional actions.

Insurance Functions — Insurance functions include underwriting, premium rating and other activities related to creation, renewal or replacement of contracts or benefits and ceding, securing or placing a contract of reinsurance for risk related to health care claims (including stop-loss and excess-loss coverage).

Line of Business (LOB) — Refers to the particular types of coverage that are marketed by a plan.

Medical Identity Theft — Using another's identity to get medical care or drugs.

Minimum Necessary — The least amount of PHI necessary to achieve the purpose of a use or disclosure.

Operations — Health care operations include insurance functions, such as determination of benefits and customer service; business functions, such as auditing and accounting activities; and quality assurance functions, such as provider accreditation.

Payment — Payment functions include activities related to the collection of premiums, including the determination of premiums, and the payment of claims.

Personally Identifiable Information (PII) — PII rules apply to federal government contractors. This is information that can be used to uniquely identify, contact or locate a single person or can be used with other sources to uniquely identify a single individual. Some examples of PII are name, address, Social Security number, telephone number, email address and birthdate.

Phishing — The use of fraudulent email requesting verification of information or passwords. It contains warning of a dire consequence if verification is not completed. The email usually contains a link to a website that looks legitimate, with company logos and content, and has a form requesting entry of a password or other secure information.

Pretexting — The use of an invented scenario to try to get secure information. A caller uses known information (birthdate, address, etc.) to add legitimacy to the request for more detailed information or passwords.

Protected Health Information (PHI) — Health-related information that identifies the individual or could be used to identify the individual who is the subject of the information that is transmitted or stored in any form or medium (including electronic records, paper records and oral communications). This includes information that relates to:

1. The past, present or future physical or mental health condition of an individual.
2. The provision of health care to an individual.
3. An individual's payment for the provision of health care.

What constitutes PHI must be determined on a case-by-case basis; however, to be safe, it is best to assume that names, addresses, telephone numbers, account numbers, birthdates, Social Security numbers, and any health records or health insurance records are examples of PHI.

Ransomware — A type of malware that prevents or limits users from accessing their computer system, either by locking the system's screen or by locking the users' files unless a ransom is paid. More modern ransomware families, collectively categorized as crypto-ransomware, encrypt certain file types on infected systems and force users to pay the ransom through certain online payment methods to get a decrypt key (usually in an untraceable payment form like Bitcoin).

TPO — Acronym for treatment, payment and health care operations, which is generally used in reference to those activities undertaken by BlueCross in which it is allowed to use or disclose a member's PHI without authorization.

Treatment — The provision, coordination or management of health care and related services by health care providers.

Vishing — The fraudulent practice of making phone calls or leaving voice messages purporting to be from reputable companies to induce individuals to reveal personal information, such as bank details and credit card numbers.

Whaling — A specific form of phishing or spear-phishing. It targets upper management in private companies. The objective is for upper management to divulge confidential company information. Whaling involves a webpage or an email with a link or attachment that masquerades as legitimate and urgent. The content of a whaling attack is tailored for upper management and usually involves some kind of falsified companywide concern.

How To Report a Concern

- Talk to your immediate supervisor, your next level of management or another leader in your division.
- Call a compliance officer:

Corporate Compliance Officer	Louis M. McElveen	800-288-2227, ext. 43435
Medicare Advantage and Federal Marketplace	Joel Pierstorff	800-288-2227, ext. 41971
Celerian Group	Cindy Cooper	800-288-2227, ext. 38710
- CGS Administrators	Linda Martin	615-782-4568
- Companion Data Services	Taliah Jarvis	800-288-2227, ext. 48537
- Palmetto GBA	Lee McElveen	800-288-2227, ext. 38143
- PGBA, InStil and Medicaid Division	Jennifer Mashura	800-288-2227, ext. 36623

- **ANONYMOUS** — Call the Corporate Compliance Hotline at **888-263-2077**.
- **ANONYMOUS** — Go to the compliance hotline website at **www.WebReportingHotline.com**.
- **ANONYMOUS** — Select the **Report Compliance Concerns** link under Company Areas, Corporate Audit, Compliance & Ethics.
- Send interoffice mail to the corporate compliance officer (AC-200).
- Contact the HR Support Center at 800-288-2227, ext. 46654.
- If you need to report suspected fraud, waste or abuse by an employee, provider, member, vendor or other external entity, you can contact the fraud hotline at 800-763-0703.

Notes