South Carolina

# Compliance Overview and Our Values


Ways to Report a Concern:
- Compliance Hotline - 888-263-2077
- Compliance Website - WebReportingHotline.com

Revised 07/19

# Compliance Overview and Our Values

# 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,

David Pankau, President and CEO

# Disclaimer

If you are an employee of a contractor, nothing herein shall be construed to change this relationship or to make you an employee of BlueCross BlueShield of South Carolina and/or any of its subsidiaries or affiliates.

If you are an employee of BlueCross BlueShield of South Carolina and/or any of its subsidiaries or affiliates, please note that all employees of BlueCross BlueShield of South Carolina and any of its subsidiaries or affiliates are employed at-will and may quit or be terminated at any time and for any reason. Nothing in any of BlueCross BlueShield of South Carolina's rules, policies, handbooks, procedures or other documents relating to employment creates any express or implied contract of employment. No past practices or procedures, whether oral or written, form any express or implied agreement to continue such practices or procedures. No promises or assurances, whether written or oral, which are contrary to or inconsistent with the limitations set forth in this paragraph create any contract of employment unless: 1) the terms are put in writing, 2) the document is labeled "contract," 3) the document states the duration of employment and 4) the document is signed by the chief executive officer.

Printed Name of Employee/Contractor

Employee's/Contractor's ID

Employee's/Contractor's Signature

Date

Version 1

# Disclaimer

If you are an employee of a contractor, nothing herein shall be construed to change this relationship or to make you an employee of BlueCross BlueShield of South Carolina and/or any of its subsidiaries or affiliates.

If you are an employee of BlueCross BlueShield of South Carolina and/or any of its subsidiaries or affiliates, please note that all employees of BlueCross BlueShield of South Carolina and any of its subsidiaries or affiliates are employed at-will and may quit or be terminated at any time and for any reason. Nothing in any of BlueCross BlueShield of South Carolina's rules, policies, handbooks, procedures or other documents relating to employment creates any express or implied contract of employment. No past practices or procedures, whether oral or written, form any express or implied agreement to continue such practices or procedures. No promises or assurances, whether written or oral, which are contrary to or inconsistent with the limitations set forth in this paragraph create any contract of employment unless: 1) the terms are put in writing, 2) the document is labeled "contract," 3) the document states the duration of employment and 4) the document is signed by the chief executive officer.

Printed Name of Employee/Contractor

Employee's/Contractor's ID

Employee's/Contractor's Signature

Date

EMPLOYEE COPY

Version 1

BlueCross BlueShield of South Carolina and Its Subsidiaries

# HIPAA/Compliance/Rules of Behavior/ Security Awareness Attestation

OUR Values

Instructor: _____ Location: _____

Date of Class: _____ Time: _____

Name: _____ BlueCross ID: _____

I hereby attest that I have received, read and understood the course listed above and will comply with the Corporate Code of Conduct, which includes Privacy and Security Rules, the Rules of Behavior and other laws that affect our business.

_____ _____

Signature Date

# Our Values

Date of Class:_____ Instructor: _____ Location: _____

Instructions: To continue to provide you with quality training programs, we request your honest input on this evaluation. Please rate this program by **circling** your response.

| | | | |
|---|---|---|---|
| 1. The questions and cases reviewed during this program enhanced my learning experience. | Disagree | Neutral | Agree |
| 2. I have a better understanding of the role of management and other resources in reporting concerns, even if they are not compliance-related. | Disagree | Neutral | Agree |
| 3. The instructor was responsive to participants and answered clearly. | Disagree | Neutral | Agree |
| 4. The instructor demonstrated knowledge and understanding of the topic and/or offered to find out the answer. | Disagree | Neutral | Agree |
| 5. The course was beneficial to me in understanding our compliance program. | Disagree | Neutral | Agree |

6. What did you like most about the course? _____

_____

_____

_____

7. What did you like least about the course? _____

_____

_____

_____

8. What changes would you suggest to improve the effectiveness of this course? _____

_____

_____

_____

This is not a contract of employment. If you are an employee of BlueCross BlueShield 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 reasons.

# Background

**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 2009 the "Data Breach Rule" was added, which dictates notice requirements when a breach of unsecured PHI has occurred. Under this rule, we may have to notify each affected individual, Health and Human Services (HHS) and, in some cases, the media, of any breach that either we or our business associates experience.

In 2013, the final omnibus rule was released, which includes additional HIPAA requirements for our company and its business associates. Further limits were set on how we are permitted to use PHI for marketing and underwriting. Any changes in requirements that might affect how you do your job will be included in your area's procedures.

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

- In the Corporate Policies section found in OurHRConnect.
- In the HIPAA Privacy Operational Requirements document located on the Privacy Information page of My e-Work, under Privacy and Security.

Whether you are an in-house, off-site or remote location employee, you should review and become familiar with these policies, since they apply to all employees.

### How do they affect BlueCross?

BlueCross deals with a tremendous amount of PHI on a daily basis, either electronically, on paper or by phone. Federal law directs us to comply with HIPAA rules and regulations. See the definition of PHI in the Glossary in the back of this booklet.

Many of our government programs areas also reference the term "personally identifiable information" (PII). This section discusses PHI as it relates to the HIPAA Privacy rule. But for most government contracts, these rules also apply to PII. See the definition of PII in the Glossary in the back of this booklet.

PII includes information that can be used to identify a person, such as the person's name, address or account ID and username. 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 user names to be PII and employees should protect this information accordingly.

The Privacy Rule protects all PHI in any form or media, whether electronic, paper or oral.

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.

BlueCross requires that all employees and its 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 all specialized training.
- 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 office must document and retain a record of the initial HIPAA training for six years.

## *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 all corporate activities with privacy implications. He also monitors all 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 has an assigned privacy official who coordinates with the Corporate Privacy office. You can find a complete list of privacy officials in the company on My e-Work under Privacy and Security.

## Security council

Elizabeth C. Hubbard chairs the BlueCross Corporate Security Council, a centralized governing body that addresses the subject of electronic protected health information (ePHI) and other sensitive information. The Security Council ensures that BlueCross complies with a basic level of security that the chief information officer (CIO) approves, as well as security requirements due to legislative requirements, contractual commitments or other externally imposed obligations. The Security Council develops and implements appropriate administrative, technical and physical safeguards to protect the ePHI in our custody from threats or hazards to the security or integrity of the information or misuse or improper disclosures of ePHI.

## Uses and disclosures

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. See the definition of TPO in the Glossary in the back of this booklet.

## Authorization to disclose 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.

## 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, prior to disclosure, you must know the reason for the request or the intended use of the information.

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.

## *Confidential or sensitive information*

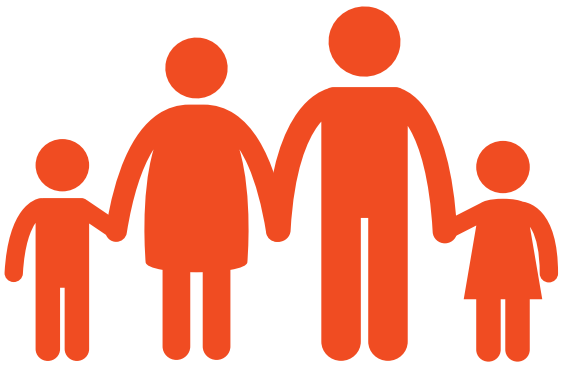
Information is considered sensitive if the loss of confidentiality, integrity or availability could be expected to have a serious, severe or catastrophic adverse effect on organizational operations, organizational assets or individuals. PII is a subset of sensitive information and is defined as data that can potentially be used to identify, locate or contact an individual, or potentially reveal the activities, characteristics or other details about a person. You are responsible for learning and understanding how to recognize and identify confidential/sensitive information.

- 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.
- Never knowingly or willingly conceal, remove or falsify information.
- Never destroy confidential or sensitive information in an improper or unapproved manner.
- You are not permitted to use company or customer information for non-business or personal purposes.

## *Individual's rights*

The HIPAA Privacy Rules ensure 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.



# Safeguarding PHI

## *Safeguarding 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 content 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 the use of approved recycling/shred bins.
- Follow your area's specific procedures for marking documents according to the data classification.

## *Electronic data safeguards*

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 by pressing Ctrl, Alt, Delete and then click on "Lock Workstation" or press the Windows key and "L."
- When you are ready to leave work for the day, close out your applications, click on the START button at the lower left-hand side of the screen and select "Restart" from the menu. This allows software updates, etc., to be loaded to your computer overnight.
- All corporate-owned laptop computers must have approved full disk encryption software installed and active.
- Follow your area's procedures for work-at-home workstations, 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 taken out of the office, protect the computer with a locking cable or secure it out of sight.
- Do not 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.
- Do not install or use an unapproved desktop modem or analog line.
- 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 LMS, as well as 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.

### Workstation and PHI security — remote access

Simply scrambling PHI that you are emailing to prevent someone from identifying the information is known as very weak encryption. Some Windows programs, such

as Excel, have this type of encryption capability. We are not permitted to use scrambling of PHI for purposes of encryption. We cover how to properly encrypt email later in this document.

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.

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

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

Do not store sensitive information in public folders or other insecure physical or electronic storage locations.

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 OS will use line of business 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 messaging or non-company owned instant messaging application.
- 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 them with the method of accessing email, and tell them if any abnormal activity has been observed.

Do not install personal software on company workstations or use company workstations for personal use.

Do not duplicate or distribute information or data protected by a copyright law — including music, software, documentation and other copyrighted materials — without documented approval from management, the manufacturer, licensee or applicable site license agreement.

Computers and consumer electronic devices used to connect to systems from a remote location are not backed up. Do not store any PHI or other confidential/sensitive information on a laptop or work-at-home computer without prior management approval.

Do not use personally owned computers or portable devices such as laptops or non-company devices (USB drives) to access, store or process business-related PHI or other confidential/sensitive information without authorization and appropriate safeguards.

Do not direct or encourage others to use another person's account, identity or password.

Do not allow others to use your account, identity or password.

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).

Only permit authorized users to use company equipment and/or software.

### PHI Safeguards — Internet and Email Security

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.

Assume that mail on the internet is not secure. Never put in an email message anything you would not want printed in a newspaper.

Use an approved and authorized encryption tool to encrypt any sensitive information that you must transmit over the internet.

The company never allows the exchange of chain letters, pornographic material or material deemed offensive to others. Offenders are subject to disciplinary action. The company never allows the sending or posting of threatening, harassing, intimidating or abusive material about others in public or private messages or forums.

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 (instant messaging software) without proper authorization.
- Operating unapproved websites.
- Incurring more than minimal additional expense, such as using non-trivial 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 that you download from the internet will be scanned for computer viruses.

Most BlueCross BlueShield of South Carolina employees, with exceptions listed in the next two paragraphs, can send PHI via Microsoft Outlook to someone outside BlueCross or its subsidiaries by adding [SECURE] at the beginning of the email subject line and including 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 internally. This will not work externally from an internal source.

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.

### 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 including at least one number, one special character, and at least one capital letter. Special characters are limited to @, # or $. In some areas these requirements may 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.
- Do not use personally owned or noncompany-issued devices to access, process or connect to the company's network or systems.
- Change your password when the system requires it. The 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).

### Logon monitoring

- User IDs will be revoked after the third incorrect logon attempt.
- You should not store PHI on local drives or removable media unless there is a specific business need to do so. If PHI is stored on removable media, you must encrypt the data. It is best to store this type of information on the network in a secure location.
- 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.

### Termination/Transfer Security

- If you are in management, you must complete the payroll termination form prior to, 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.
- Upon termination, management must collect all I/S-related, company-owned property from the terminated employee.
- 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, multiple users share the faxgate number. If one of the users either leaves the company or transfers to another area of the company, you must change the password for the faxgate.

### Social Media

Social media includes all means of communicating or posting information or content of any sort on the internet, including, for example, to your own or someone else's web log or blog, journal or diary; 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 company-maintained or related PHI, PII, trade secrets or information subject to the company's attorney-client privilege, as well as information related to the company's members, subscribers, vendors or customers.
- 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 Communications.
- You should not use personal social media during work time, or on equipment the company provides unless it is work related, authorized by your manager, or otherwise consistent with company policy. Use of social media network sites is monitored.
- You should not post inappropriate material that includes discriminatory remarks, harassment, maliciously false information and/or threats of violence or similar conduct.

### Insider threat

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. 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:

- Persons attempting to acquire accesses not needed for their jobs.
- Persons bullying or harassing coworkers to give them information.
- Persons who are disgruntled or have shown inordinate, long-term job dissatisfaction.
- 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 that an insider threat may exist, you should report them to your manager, Compliance, Security or Human Resources. You can also report concerns using the hotline (888-263-2077) or the internet (www.webreportinghotline.com). Please be sure to include enough information so the company can investigate the issue.

### Social engineering

Beware of social engineering scams designed to convince you that you are required to reveal your password or other secure information. Remember, the TSC should NEVER ask you for your password.

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

Phishing is the use of fraudulent email requesting verification of information or passwords. It contains warning of a dire consequence if you don't complete verification. 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.

Whaling is 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.

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

These tactics rely on your desire to be helpful. Always be cautious when sharing any information, no matter how innocent it may seem.

### Phishing emails

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.

- Question the authenticity of the email.
- Don't reply to the email.
- Don't click on any links in the email.
- Don't open or save any attachments in the email
- Forward it to email address Junk.Email@bcbssc.com.
- Right click on the sender's name, scroll down to "Junk" and click on "Block Sender."
- Delete the unwanted email.

If you accidentally click on a link or open an 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 and change your password immediately through the correct channels.

### Information Spillage

Information spillage refers to sensitive information being transferred to another information system, unintentionally or otherwise, that is not designated or does not have the proper authorization to retain such information. Information spillage typically occurs when information that is not believed to be sensitive is transferred or placed on a non-authorized information system. The data is then discovered or deemed to be sensitive while being housed on an information system that is not authorized to contain such information. This also may be considered a breach.

If information spillage is suspected, please contact the TSC and notify your manager immediately.

### Protection from malicious software

A virus is one type of malicious software within a program that reproduces itself in other executable code during normal processing. 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 mainframe gateways. We use a current anti-virus program on all company-owned computers. Do not disable or interrupt anti-virus scans or other approved security mechanisms and software.

Potential virus warning signs include:

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

### To Protect Against Viruses

- The company strictly prohibits the use of personal software on corporate-owned workstations. Copying and using someone else's software violates copyright and licensing laws.
- If you suspect a computer virus, do NOT shut down your computer. Immediately contact the TSC.
- If you receive an email that appears suspicious, do not open it or any attachments. Forward the email to Junk.Email, block the sender and then delete the email.
- Ensure that software, including downloaded software, is properly licensed, free of malicious code and authorized before installing and using it on company systems.

## *Physical security/piggybacking*

Access to all locations must be controlled. The following points regarding ID badges apply to those locations with security card access systems installed. However, the need for controlled access applies to any restricted location.

- You are required to present your ID card to a security officer at an approved building entrance, scan your own ID badge when entering a secured facility and wear your badge so it can be seen while inside any secured facility.
- Never allow another individual to enter any secured facility on your ID badge. This is called "piggybacking" and is against BlueCross corporate policy.
- You should politely challenge any individual who does not have an approved ID badge displayed. You should escort individuals without badges to the nearest security station for assistance.
- If your badge does not allow you access, you should proceed outside of the building to the main entrance to the security desk to get appropriate access.
- When you leave 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.
- 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, go to Security and follow established procedures to get a temporary badge.

A piggybacking violation has occurred when:

- You allow someone to enter behind you without swiping his or her badge.
- You follow someone in without swiping your own badge.
- You witness someone piggybacking and don't report it.

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:

- 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.
- No employee or visitor may enter a facility by following an employee in, or by having an employee open the door.
- When following someone into a door that requires card access, employees should allow the door to close fully before swiping their card to enter.
- Employees must wear 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.
- When employees lose a badge or leave badges at home, a manager must sign them in and arrange a temporary badge for the day. 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.

If you witness a person attempting to piggyback, ask the person to follow you to the nearest security desk for assistance. If the person refuses or walks away, contact Security as soon as possible.

## *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 privacy official must report it to the Privacy office. If an area does not have a privacy official, then management should immediately report the disclosure to the 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.

Here are some examples of 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

You should immediately report known or suspected privacy and security violations to your management and the TSC at ext. 42352 (800-288-2227, ext. 42352) or 877-363-8896. Management is to report it to the LOB privacy official and/or Compliance Unit for its area or the Privacy Office. If management does not take adequate action immediately, you can notify the Corporate Privacy officer or your area's privacy officer, call the compliance hotline at 888-263-2077, visit www.webreportinghotline.com, or visit My e-Work and select Report Compliance Concerns, if you want to remain anonymous.

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.

## *PII — additional information*

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

Federal privacy provisions require contractors 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, 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 ensure fairness in making those determinations.

Only use PII for the purposes for which it was collected.

## *Privacy and security rules violations*

### Penalties for Violations

If you violate the Privacy and Security Rules, you will be subject to disciplinary action, up to and including termination. Additionally, you and/or BlueCross could be subject to civil monetary penalties up to $1.5 million for identical violations during a calendar year, and criminal penalties of $250,000 and 10 years imprisonment per violation can be imposed.

Since January 2017, The U.S. Department of Health & Human Services, Office for Civil Rights has reached settlements with several covered entities for amounts ranging from $31,000 (for not having a business associate agreement) to $16 million (for multiple violations).

### Security Violations

- Violations of corporate security policies can result in termination for a first offense.
- Do not direct or encourage others to violate policies.
- Immediately change your password, notify your management and the TSC if you believe someone has learned your password.
- Immediately report known or suspected system problems and violations that could lead to the unauthorized disclosure, alteration or destruction of sensitive data to management, the TSC and/or your Privacy official. You can also call the compliance hotline at 888-263-2077, log on to www.webreportinghotline.com or visit My e-Work and select Report Compliance Concerns, if you want to remain anonymous.

## *Member complaint process*

A complaint from a member (not an employee) related to privacy and security must be sent to the Corporate Compliance/Privacy office for investigation and response.

The Privacy office will document each complaint and its disposition. The Privacy staff will enter the information into a database and keep that information for at least six years.

Some of the subsidiaries may have additional processes, and their employees should also contact their company privacy officer.

## *Changes to privacy and security rules*

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 Law department and the Security Council, will track material changes to the Privacy and Security Rules. They will recommend changes to corporate policies and procedures as necessary to comply with changes in the law.

For more information on HIPAA privacy and security, visit OurHRConnect on My e-Work. Click on Corporate Policies and view policy number 65019 – HIPAA Privacy Policy.

## *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 government regulatory and investigative agencies. We may be asked to cooperate with a government investigation or to respond to a request for information about company business. The request may come directly to management, or you may be contacted individually. If a government investigator contacts you at home or at work, here are some things you should know.

The investigator 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!

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.

## *How to respond if you are contacted by a federal or state agency representative for information regarding company business (continued)*

If you receive a subpoena, immediately notify your management and the Law department.

Note — Some employees associated with PGBA and Medicare may 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 and 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. As consumers, this translates to higher premiums for all of us.

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.

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 by its own employees. Penalties and consequences of fraud and abuse are just as harsh and detrimental to the company and its employees as they are to providers or others when caught.

Because of this, it is important you understand the difference between fraud 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.

**Abuse** — Improper and excessive use of benefits or services by providers or members. Abuse may 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.

**The effects of fraud and abuse include:**

- Increased health care costs due to uncovered fraudulent expenses.
- Lost business opportunities/contracts, thus 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 are subject to the penalties for fraud, including providers, members, employees and vendors.

**Penalties for fraud include:**

- Potential monetary penalties ranging from $11,181 to $22,363 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. These laws are designed to help us deal with and control fraud and abuse:

## *Fraud and abuse and related federal laws (continued)*

These laws are designed to help us deal with and control fraud and abuse:

**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 the federal government or its agents to pay or approve a false or fraudulent claim. It also protects individuals from retaliation for reporting suspected fraud and abuse.

**Anti-Kickback Statute** — This provides penalties for individuals or entities that knowingly and willfully offer, pay, solicit or receive remuneration to induce or reward business payable under the Medicare or other federal health care programs.

**Sarbanes Oxley Act of 2002 (SOX)** — This creates better corporate control environments and makes executives personally accountable for internal control over financial reporting. Even though SOX does not apply to companies that are not publicly traded (like BlueCross), we are required to comply with the National Association of Insurance Commissioners Model Audit Rule (MAR), which is the private insurance industry's version of SOX. BlueCross had to begin meeting the requirements of MAR in January 2010. The compliance effort began in 2007 and we are performing the tasks to ensure compliance on an annual basis.

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.

**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."

# Compliance

### Introduction to *Our Values*

As you know, the Corporate Compliance program and our Code of Conduct, *Our Values*, guides all of us to do the right thing. We are committed to conducting business the right way. These 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.

What you may not realize is that our Compliance department and corporate and Government Programs 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 continue to stay on course and succeed as individuals and as 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 calls to the 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 that 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 mission*

Our mission is to create value for our members, customers, employees and communities through maintaining a fiscally strong, high quality organization. We accomplish this through excellence in service; offering efficient and affordable insurance plans and administrative services products; by being the nation's pre-eminent supplier of high quality, efficient services for PGBA and Medicare; and by using our expertise in information technology and financial services to support and acquire other profitable businesses.

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

So, what will we use to guide us on this journey? Here is the foundation for our values:

# Our Values

## *Communication*

- We will support open communication between 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 have access to.
- 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
  - PII/PHI
  - Electronic claims, claims histories, enrollment, referrals, authorizations and other claim-related information
  - Rate adjustments
  - Pricing information
  - Underwriting procedures
  - RACF account numbers and passwords
  - Information about our business partners
- We will protect and preserve things that belong to the company, including our offices, 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 impact 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, doesn't mean it is 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, 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.

## *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 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 to not 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, Human Resources and/or through work enrichment programs that may be available in our division.
- 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.

All employees (full-time, part-time and temporary), contractors, and consultants are required to receive training on *Our Values* on their first day of hire before reporting to their work areas. Recurring annual compliance training is also mandatory for all employees, contractors and consultants. We want to make sure you understand this program — how it works and how it affects you. You can play an active part in improving our company!

**Please keep your personal copy of *Our Values* in a ready, safe place. It is an important document for you to use as a reference. You should read the contents carefully and follow all its guidelines. Please note that this booklet does not change your employment relationship with the company.**

# Corporate Policies That Relate To *Our Values*

## *Gifts and social/professional functions*

We will avoid any situation where a conflict of interest could exist, or appear to exist, between our personal interests and the business interests of the company. These guidelines on gifts and social/professional functions will help you determine when a conflict of interest may exist. 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 area's Compliance department.

This policy applies to all gifts and social/professional functions associated with your work. Gifts you give and 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, non-business reasons, even though you may have work associations with the recipient.

## *Gifts you can keep*

Usually, a gift with a value of $100 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 (COI) form. Some examples of such gifts are logo items from other companies, like umbrellas, keychains, flashlights, tote bags or a windbreaker. Certificates, plaques and other award-type items are also acceptable. Flowers, candy and other food items are acceptable, as well.

Keep in mind, 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 COI 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 COI form. You must also get approval from your management before accepting the gift that puts the annual value of all gifts at more than $100.

EXCEPTION: Government program (Medicare, PGBA and Medicaid) subsidiary employees, contractors and consultants have a $50 gift limit. They CANNOT accept ANYTHING of value from anyone or any entity that bills or receives funds from the Medicaid, Medicare or PGBA programs (i.e., doctors, hospitals, vendors, medical suppliers, beneficiaries, home health agencies, hospices, etc.). See your subsidiary's supplemental government programs compliance handbook or departmental policies for additional information.

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 can give to others*

Company logo items of minimal value are acceptable gifts for outside contacts. Certificates of appreciation or recognition are also appropriate gifts you may give. Refreshments provided at meetings or light lunches served to a meeting group are also acceptable. You can give federal and state employees these token items and limited refreshments; however, federal and state employees cannot accept any other gifts.

## *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 you should not accept it. If you are not comfortable with receiving a gift, don't accept it.

## *Gifts you cannot give others*

Cash gifts are always inappropriate, and you cannot offer them 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*

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 an outside source pays the cost of your attendance. Be sure to check with your management before attending.

## *Political activity and contributions*

- 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 Government Affairs division at 800-288-2227, ext. 44770, for advice.

## *Jobs outside the company*

BlueCross encourages all employees to support community programs that reflect positively on the company. 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) will be required to complete a COI form. The form 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 course of the year, it is your responsibility to immediately notify your management and fill out a new COI form by contacting COI.FORM@bcbssc.com. They will initiate the COI for your completion in OurHRConnect.

## *Telephone and workstation monitoring*

All company telephones and workstations are subject to being recorded or monitored by area management or by Corporate Audit 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.

# 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 *Our Values* 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 *Our Values* or any requirements or responsibilities on your part, we encourage you to discuss them with your manager, the Corporate Compliance officer or, if you are a government programs employee, your area'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, visit My e-Work to review the corporate policies online. 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 the *Our Values* code of conduct, as well as potential violations of federal, state and local laws and regulations. We are committed to looking into your concerns and addressing them if we find they 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?

First, talk to 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. If the issue still is not resolved to your satisfaction, or if you are not comfortable talking to your manager or another management person in your division, contact the Corporate Compliance officer, Louis M. McElveen, at 800-288-2227, ext. 43435.

In addition, if you work in a government programs area or Companion Data Services (CDS), you can contact your company's compliance officer. The Compliance Directory is on My e-Work under Corporate Audit, Compliance, Ethics.

You can also contact someone from Employee Relations in Human Resources at 800-288-2227, ext. 41927, or your Human Resources generalist 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 hotline or directly to one of the compliance units that is an employee relations matter (such as tardiness, job selections, dress code, sexual harassment, etc.), these will be referred to the Human Resources department for appropriate handling.

## Anonymous reporting

If you wish to remain anonymous, you can also contact the Corporate Compliance office through our special hotline at 888-263-2077. This number is not an inside phone number. We have hired a special compliance company to handle these calls. The company we contract with 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 getting this information. Your report can truly be made without the company identifying you. When you call the compliance hotline, you'll receive a call-back date and a reference number in case additional information is needed.

You can also remain anonymous by visiting My e-Work and selecting Report Compliance Concerns, or you can visit www.webreportinghotline.com from any computer. This website is 100 percent anonymous. The same independent company that manages our compliance hotline hosts the website. You can also send an anonymous note via interoffice mail to Corporate Compliance or use the drop box if employed in government programs.

We will make every attempt to investigate issues reported through regular channels or anonymously. Be aware that if you do not provide enough information in your anonymous report, it may limit our ability to conduct an investigation and could lead to no corrective action being taken. In cases such as these, we may not be able to substantiate your anonymous report, and we would not be able to contact you for more information. 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 decide to contact a compliance staff person directly, we understand you may prefer to remain anonymous. Although we try to protect the confidentiality of persons who have reported suspected misconduct directly to a compliance unit, we cannot guarantee confidentiality. 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. We have 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 for a first offense. We are committed to protecting employees who make good-faith reports of compliance concerns.

## *Nonretaliation*

Our nonretaliation policy 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. 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 may 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. Keep in mind, however, that retaliation does not include appropriate disciplinary action against an employee who may have engaged in wrongdoing or who is not meeting expectations.

Employees will not be exempt from the consequences of their wrongdoing because they reported the wrongdoing. Nor will employees be exempt from the consequences of their inadequate performances because they reported a wrongdoing. The consequences from that wrongdoing or inadequate performance, however, 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.

## *Whistle-blower protection*

Federal agencies and their contractors must protect government contractor employees who act as "whistle-blowers." 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:

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

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. We are 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:**

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

**Management will not:**

- Ignore reports or questions regarding compliance concerns or issues.
- Retaliate against or harass in any way any employee or person who raises a compliance issue or concern.
- 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.

# Diversity Statement

At BlueCross BlueShield of South Carolina and its subsidiary companies, diversity refers to the collective mixture of differences and similarities. We understand that 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; as well as our workplace culture. For BlueCross BlueShield of South Carolina, diversity matters!

The *Our Values* program is very important to the company and to our ability to continue to provide a quality workplace for you and for all the various customers we serve. We are committed to and believe in our code of conduct — it is the right way to do business!

# Glossary

**Abuse** — Improper and excessive use of benefits or services by providers or members. Abuse may 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** — 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.

**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 (PII) and/or protected health information (PHI).

**Individually Identifiable Health 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.

**Insurance Functions** — Underwriting, premium rating and other activities related to the 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)** — Particular types of coverage that are marketed by a plan.

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

**Operations** — 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** — Activities related to the collection of premiums, including the determination of premiums, as well as the payment of claims.

**Personally Identifiable Information (PII)** — Information that can be used to uniquely identify, contact or locate an individual or that can be used with other sources to uniquely identify an individual.

**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

**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 that 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 in order 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.

South Carolina



Stock #: 56284

210893-7-2019