Remove Watermark Now

Changes Rehabilitation LLC

HIPAA Manual

HIPAA/HITECH Omnibus Final Rule

pdfelement

Remove Watermark Now

HIPAA Policies and Procedures

Updated: 7/30/18

Table of Contents

HIPAA1	General HIPAA Compliance
HIPAA2	Policies and Procedures
HIPAA3	Documentation
HIPAA4	Documentation Retention
HIPAA5	Documentation Availability
HIPAA6	Documentation Updating
HIPAA7	HHS Investigations
HIPAA8	Breach Notification
HIPAA9	Privacy Officer
HIPAA10	State Law Preemption
HIPAA11	HIPAA Training
HIPAA12	PHI Uses & Disclosures
HIPAA13	Patient Rights
HIPAA14	Complaints
HIPAA15	Risk Mitigation Process
HIPAA16	Risk Analysis
HIPAA17	Risk Management Implementation
HIPAA18	Sanction Policy
HIPAA19	Information Systems Activity Review
HIPAA20	Assign Security Responsibility
HIPAA21	Authorization & Supervision
HIPAA22	Workforce Clearance
HIPAA23	Access Termination
HIPAA24	Access Authorization
HIPAA25	Access Establish and Modify
HIPAA26	Security Reminders
HIPAA27	Malware Protection
HIPAA28	Log-in Monitoring
HIPAA29	Password Management
HIPAA30	Security Incident
HIPAA31	Data Backup
HIPAA32	Disaster Recovery
HIPAA33	Emergency Mode Ops
HIPAA34	Testing & Revision
HIPAA35	Criticality Analysis
HIPAA36	Evaluation
HIPAA37	Business Associates
HIPAA38	Contingency Ops
HIPAA39	Facility Security
HIPAA40	Access Control
HIPAA41	Maintenance Records
HIPAA42	Workstation Use
HIPAA43	Workstation Security
HIPAA44	Media Disposal
HIPAA45	Media Re-Use
HIPAA46	Hardware & Media Accountability
HIPAA47	Data Backup & Storage
HIPAA48	Unique User ID
HIPAA49	Emergency Access
HIPAA50	Automatic Log-Off
HIPAA51	Encryption & Decryption

Pdfelement

HIPAA52	**Audit Controls**
HIPAA53	**Integrity Controls**
HIPAA54	**Person or Entity Authentication**
HIPAA55	**Transmission Security**
HIPAA56	**Mobile Device**

Remove Watermark Now

pdfelement

Remove Watermark Now

HIPAA1-General HIPAA Compliance Policy

Updated: 7/30/18

Introduction

CHANGES REHABILITATION LLC. has adopted this General HIPAA Compliance Policy in order to recognize the requirement to comply with the Health Insurance Portability and Accountability Act ("HIPAA"), as amended by the Health Information Technology for Economic and Clinical Health ("HITECH") Act of 2009 (Title XIII of division A and Title IV of division B of the American Recovery and Reinvestment Act "ARRA") and the HIPAA Omnibus Final Rule (Effective Date: March 26, 2013). We acknowledge that full compliance with the HIPAA Final Rule is required by or before September 23, 2013.

CHANGES REHABILITATION LLC. hereby acknowledges our duty and responsibility to protect the privacy and security of Individually Identifiable Health Information ("IIHI") generally, and Protected Health Information ("PHI") as defined in the HIPAA Regulations, under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under principles of general and professional ethics. We also acknowledge our duty and responsibility to support and facilitate the timely and unimpeded flow of health information for lawful and appropriate purposes.

Scope of Policy

This policy governs General HIPAA Compliance for **CHANGES REHABILITATION LLC.** All personnel of **CHANGES REHABILITATION LLC.**must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

pdfelement

Assumptions

- **CHANGES REHABILITATION LLC.** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA Regulations.
- **CHANGES REHABILITATION LLC.** must comply with HIPAA and the HIPAA implementing regulations, in accordance with the requirements at 45 CFR Parts 160 and 164, as amended.
- Full compliance with HIPAA is mandatory and failure to comply can bring severe sanctions and penalties. Possible sanctions and penalties include, but are not limited to: civil monetary penalties, criminal penalties including prison sentences, and loss of revenue and reputation from negative publicity.
- Full compliance with HIPAA strengthens our ability to meet other compliance obligations, and will support and strengthen our non-HIPAA compliance requirements and efforts.
- Full compliance with HIPAA reduces the overall risk of inappropriate uses and disclosures of Protected Health Information (PHI), and reduces the risk of breaches of confidential health data.
- The requirements of the HIPAA Administrative Simplification Regulations (including the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules) implement sections 1171-1180 of the Social Security Act (the Act), sections 262 and 264 of Public Law 104-191, section 105 of 492 Public Law 110-233, sections 13400-13424 of Public Law 111-5, and section 1104 of Public Law 111-148.
- Entities subject to HIPAA Rules are also subject to other federal statutes and regulations. For example, federal programs must comply with the statutes and regulations that govern them. Pursuant to their contracts, Medicare providers must comply with the requirements of the Privacy Act of 1974. Substance abuse treatment facilities are subject to the Substance Abuse Confidentiality provisions of the Public Health Service Act, section 543 and its regulations. And, health care providers in schools, colleges, and universities may come within the purview of the Family Educational Rights and Privacy Act.

Policy Statement

- It is the Policy of **CHANGES REHABILITATION LLC.**to become and to remain in full compliance with all the requirements of HIPAA.

- It is the Policy of **CHANGES REHABILITATION LLC.**to fully document all HIPAA compliance-related activities and efforts, in accordance with our Documentation Policy.
- All HIPAA compliance-related documentation will be managed and maintained for a minimum of six years from the date of creation or last revision, whichever is later, in accordance with **CHANGES REHABILITATION LLC.**'s Document Retention policy.

Remove Watermark Now

Procedures

In accordance with the amended HIPAA Final Rule (Effective Date: March 26, 2013), **CHANGES REHABILITATION LLC.**commits to enacting, supporting, and maintaining the following procedures and activities, as a minimum, as required by HIPAA:

- **Privacy Policies and Procedures** -- **CHANGES REHABILITATION LLC.**shall develop and implement written privacy policies and procedures that are consistent with the HIPAA Rules.

- **Privacy Personnel** -- CHANGES REHABILITATION **LLC.**shall designate a privacy official responsible for developing and implementing its privacy policies and procedures, and a contact person or contact office responsible for receiving complaints and providing individuals with information on CHANGES REHABILITATION **LLC.**'s privacy practices.

- **Workforce Training and Management** -- Workforce members include employees, volunteers, trainees, and may also include other persons whose conduct is under the direct control of the **CHANGES REHABILITATION LLC.**(whether or not they are paid by **CHANGES REHABILITATION LLC.**). **CHANGES REHABILITATION LLC.**shall train all workforce members on its privacy policies and procedures, as necessary and appropriate for them to carry out their various functions.

- **Sanctions** -- **CHANGES REHABILITATION LLC.**shall have and apply appropriate sanctions against workforce members who violate its privacy policies and procedures, and/or HIPAA's Privacy and Security Rules.

- **Mitigation** -- **CHANGES REHABILITAION LLC.**shall mitigate, to the extent practicable, any harmful effect it learns was caused by use or disclosure of protected health information by its workforce or its business associates in violation of its privacy policies and procedures or the Privacy Rule.

- **Data Safeguards** -- **CHANGES REHABILITATION LLC.**shall maintain reasonable and appropriate administrative, technical, and physical safeguards to prevent intentional or unintentional uses or disclosures of protected health information in violation of the Privacy Rule and its own policies and to limit the incidental uses and disclosures pursuant to otherwise permitted or required uses or disclosures.

- **Complaints** -- **CHANGES REHABILITATION LLC.**shall establish procedures for individuals to complain about its compliance with its privacy policies and procedures and the Privacy Rule. **CHANGES REHABILITATION LLC.**shall explain those procedures in its privacy practices notice.

- **Retaliation and Waiver** -- **CHANGES REHABILITATION LLC.**shall NOT retaliate against a person for exercising rights provided by HIPAA, for assisting in an investigation by HHS or another appropriate authority, or for opposing an act or practice that the person believes in good faith violates any HIPAA standard or requirement. **CHANGES REHABILITATION LLC.**shall not require an individual to waive any right under the Privacy Rule as a condition for obtaining treatment, payment, and enrollment or benefits eligibility.

- **Documentation and Record Retention** -- **CHANGES REHABILITATION LLC.**shall maintain, until at least six years after the later of the date of their creation or last effective date, its privacy policies and procedures, its privacy practices notices, dispositions of complaints, and other actions, activities, and designations that the Privacy Rule requires to be documented.

Compliance and Enforcement

All CHANGES REHABILITATION LLC.managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **CHANGES REHABILITATION LLC.**'s Sanction Policy.

pdfelement

Remove Watermark Now

HIPAA2-Policy and Procedures
Updated 7/30/18

Introduction

CHANGES REHABILITATION LLC. has adopted this HIPAA Policies and Procedures Policy in order to recognize the requirement to comply with the Health Insurance Portability and Accountability Act ("HIPAA"), as amended by the Health Information Technology for Economic and Clinical Health ("HITECH") Act of 2009 (Title XIII of division A and Title IV of division B of the American Recovery and Reinvestment Act "ARRA") and the HIPAA Omnibus Final Rule (Effective Date: March 26, 2013). We acknowledge that full compliance with the HIPAA Final Rule is required by or before September 23, 2013.

We hereby acknowledge our duty and responsibility to protect the privacy and security of Individually Identifiable Health Information ("IIHI") generally, and Protected Health Information ("PHI") as defined in the HIPAA Regulations, under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under principles of general and professional ethics. We also acknowledge our duty and responsibility to support and facilitate the timely and unimpeded flow of health information for lawful and appropriate purposes.

Scope of Policy

This policy governs the establishment and maintenance of policies and procedures for **CHANGES REHABILITATION LLC.**All personnel of **CHANGES REHABILITATION LLC.**must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

pdfelement

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

Assumptions

- **CHANGES REHABILITATION LLC.** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA Regulations.
- **CHANGES REHABILITATION LLC.** must comply with HIPAA and the HIPAA implementing regulations, in accordance with the requirements at 45 CFR Parts 160 and 164, as amended.
- Full compliance with HIPAA is mandatory and failure to comply can bring severe sanctions and penalties. Possible sanctions and penalties include, but are not limited to: civil monetary penalties, criminal penalties including prison sentences, and loss of revenue and reputation from negative publicity.
- Full compliance with HIPAA strengthens our ability to meet other compliance obligations, and will support and strengthen our non-HIPAA compliance requirements and efforts.
- Full compliance with HIPAA reduces the overall risk of inappropriate uses and disclosures of Protected Health Information (PHI), and reduces the risk of breaches of confidential health data.
- The requirements of the HIPAA Administrative Simplification Regulations (including the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules) implement sections 1171-1180 of the Social Security Act (the Act), sections 262 and 264 of Public Law 104-191, section 105 of 492 Public Law 110-233, sections 13400-13424 of Public Law 111-5, and section 1104 of Public Law 111-148.
- Entities subject to HIPAA Rules are also subject to other federal statutes and regulations. For example, federal programs must comply with the statutes and regulations that govern them. Pursuant to their contracts, Medicare providers must comply with the requirements of the Privacy Act of 1974. Substance abuse treatment facilities are subject to the Substance Abuse Confidentiality provisions of the Public Health Service Act, section 543 and its regulations. And, health care providers in schools, colleges, and universities may come within the purview of the Family Educational Rights and Privacy Act.

Policy Statement

- It is the Policy of **CHANGES REHABILITATION LLC.**to create and implement appropriate policies and procedures as required by law and as suggested by good business practices and general business ethics

- All policies and procedures shall be updated and amended as needed or as required by law.
- All policies and procedures shall be distributed to, or made otherwise available to, the entire workforce.
- All policies and procedures shall be regularly maintained and secured, and copies shall be stored offsite with other important business records for safekeeping.
- All members of the workforce are required to read, understand, and comply with this and all other policies and procedures created and implemented by **CHANGES REHABILITATION LLC.**

Procedures

- **CHANGES REHABILITATION LLC.** shall create or revise its own HIPAA policies and procedures, consistent with all applicable HIPAA Rules and Regulations as well as with applicable State lawand statutes.
- **CHANGES REHABILITATION LLC.** shall designate a qualified individual to assume control of the policies and procedures process. This individual shall report to **the Board of Directors** and shall execute the creation or revision process in a timely manner, in order to meet the current HIPAA Compliance Deadline of September 23, 2013.
- **CHANGES REHABILITATION LLC.** shall engage its qualified legal counsel to guide or review the policies and procedures creation/revision process, and to intercede where necessary, to ensure **CHANGES REHABILITATION LLC.**'s policies and procedures meet all applicable HIPAA (and other) standards.
- **CHANGES REHABILITATION LLC.** shall internally publish its HIPAA policies and procedures, when complete, to its workforce members, and shall provide appropriate training to members of its workforce on the interpretation and implementation of its policies and procedures.

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **CHANGES REHABILTATION LLC.**'s Sanction Policy.

Remove Watermark Now
pdfelement

Remove Watermark Now

HIPAA3-Documentation Policy
Updated: 7/30/18

Introduction

CHANGES REHABILITATION LLC. has adopted this HIPAA Documentation Policy in order to recognize the requirement to comply with the Health Insurance Portability and Accountability Act ("HIPAA"), as amended by the Health Information Technology for Economic and Clinical Health ("HITECH") Act of 2009 (Title XIII of division A and Title IV of division B of the American Recovery and Reinvestment Act "ARRA") and the HIPAA Omnibus Final Rule (Effective Date: March 26, 2013). We acknowledge that full compliance with the HIPAA Final Rule is required by or before September 23, 2013.

CHANGES REHABILITATION LLC. hereby acknowledges our duty and responsibility to protect the privacy and security of Individually Identifiable Health Information ("IIHI") generally, and Protected Health Information ("PHI") as defined in the HIPAA Regulations, under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under principles of general and professional ethics. We also acknowledge our duty and responsibility to support and facilitate the timely and unimpeded flow of health information for lawful and appropriate purposes.

Scope of Policy

This policy governs the creation and maintenance of HIPAA-related documentation for **CHANGES REHABILITATION LLC.**All personnel of **CHANGESE REHABILITATION LLC.**must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

pdfelement

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

Assumptions

- **CHANGES REHABILITATION LLC.** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA Regulations.
- **CHANGESE REHABILITATIO LLC.** must comply with HIPAA and the HIPAA implementing regulations, in accordance with the requirements at 45 CFR Parts 160 and 164, as amended.
- Full compliance with HIPAA is mandatory and failure to comply can bring severe sanctions and penalties. Possible sanctions and penalties include, but are not limited to: civil monetary penalties, criminal penalties including prison sentences, and loss of revenue and reputation from negative publicity.
- Full compliance with HIPAA strengthens our ability to meet other compliance obligations, and will support and strengthen our non-HIPAA compliance requirements and efforts.
- Full compliance with HIPAA reduces the overall risk of inappropriate uses and disclosures of Protected Health Information (PHI), and reduces the risk of breaches of confidential health data.
- The requirements of the HIPAA Administrative Simplification Regulations (including the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules) implement sections 1171-1180 of the Social Security Act (the Act), sections 262 and 264 of Public Law 104-191, section 105 of 492 Public Law 110-233, sections 13400-13424 of Public Law 111-5, and section 1104 of Public Law 111-148.
- Entities subject to HIPAA Rules are also subject to other federal statutes and regulations. For example, federal programs must comply with the statutes and regulations that govern them. Pursuant to their contracts, Medicare providers must comply with the requirements of the Privacy Act of 1974. Substance abuse treatment facilities are subject to the Substance Abuse Confidentiality provisions of the Public Health Service Act, section 543 and its regulations. And, health care providers in schools, colleges, and universities may come within the purview of the Family Educational Rights and Privacy Act.

Policy Statement

Remove Watermark Now

- ❑ Officers, agents, employees, contractors, temporary workers, and volunteers who work for or perform any services (paid or unpaid) for **CHANGES REHABILITATION LLC.** must document all HIPAA-related activities that require documentation.
- ❑ All HIPAA-related documentation must be created and maintained in written form, which may also include electronic forms of documentation.
- ❑ Any action, activity or assessment that must be documented, shall be documented in accordance with this and other policies and procedures implemented by **CHANGES REHABILITATION LLC.**
- ❑ All HIPAA-related documentation must be forwarded, used, applied, filed, or stored in accordance with this and other policies and procedures created and implemented by **CHANGES REHABILITAION LLC.**
- ❑ All required HIPAA documentation shall be securely and appropriately maintained and stored in accordance with HIPAA Regulations and with **CHANGES REHABILITATION LLC.**'s policy on document retention.
- ❑ HIPAA documentation shall be made available, as needed, to all workforce members who are authorized to access it, and shall be made available to appropriate authorities for audits, investigations, and other purposes authorized or required by law.

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **CHANGES REHABILITAION LLC.**'s Sanction Policy.

pdfelement

Remove Watermark Now

HIPAA4-Documentation Retention Policy

Updated: 7/30/18

Introduction

CHANGES REHABILITATION LLC. has adopted this HIPAA Documentation Retention Policy in order to recognize the requirement to comply with the Health Insurance Portability and Accountability Act ("HIPAA"), as amended by the Health Information Technology for Economic and Clinical Health ("HITECH") Act of 2009 (Title XIII of division A and Title IV of division B of the American Recovery and Reinvestment Act "ARRA") and the HIPAA Omnibus Final Rule (Effective Date: March 26, 2013). We acknowledge that full compliance with the HIPAA Final Rule is required by or before September 23, 2013.

CHANGES REHABILITATION LLC. hereby acknowledges our duty and responsibility to protect the privacy and security of Individually Identifiable Health Information ("IIHI") generally, and Protected Health Information ("PHI") as defined in the HIPAA Regulations, under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under principles of general and professional ethics. We also acknowledge our duty and responsibility to support and facilitate the timely and unimpeded flow of health information for lawful and appropriate purposes.

Scope of Policy

This policy governs HIPAA Documentation Retention for **CHANGES REHABILITATION LLC.** All personnel of **CHANGES REHABILITATION LLC.** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

pdfelement

Assumptions

- **CHANGES REHABILITATION LLC.** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA Regulations.
- **CHANGES REHABILITATION LLC.** must comply with HIPAA and the HIPAA implementing regulations, in accordance with the requirements at 45 CFR Parts 160 and 164, as amended.
- Full compliance with HIPAA is mandatory and failure to comply can bring severe sanctions and penalties. Possible sanctions and penalties include, but are not limited to: civil monetary penalties, criminal penalties including prison sentences, and loss of revenue and reputation from negative publicity.
- Full compliance with HIPAA strengthens our ability to meet other compliance obligations, and will support and strengthen our non-HIPAA compliance requirements and efforts.
- Full compliance with HIPAA reduces the overall risk of inappropriate uses and disclosures of Protected Health Information (PHI), and reduces the risk of breaches of confidential health data.
- The requirements of the HIPAA Administrative Simplification Regulations (including the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules) implement sections 1171-1180 of the Social Security Act (the Act), sections 262 and 264 of Public Law 104-191, section 105 of 492 Public Law 110-233, sections 13400-13424 of Public Law 111-5, and section 1104 of Public Law 111-148.
- Entities subject to HIPAA Rules are also subject to other federal statutes and regulations. For example, federal programs must comply with the statutes and regulations that govern them. Pursuant to their contracts, Medicare providers must comply with the requirements of the Privacy Act of 1974. Substance abuse treatment facilities are subject to the Substance Abuse Confidentiality provisions of the Public Health Service Act, section 543 and its regulations. And, health care providers in schools, colleges, and universities may come within the purview of the Family Educational Rights and Privacy Act.

Remove Watermark Now

Policy Statement

- It is the Policy of **CHANGES REHABILITATION LLC.** to retain all HIPAA-related documentation for a minimum period of six (6) years from the date of its creation or modification, or the date when it was last in effect, whichever is later.
- HIPAA documentation shall be securely stored and maintained in a manner consistent with the HIPAA Privacy and Security Rule Standards.
- HIPAA documentation shall be made available to those workforce members who have a legitimate need for it, and who are authorized to access it, according to current HIPAA Standards.

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **CHANGES REHABILITATION LLC.**'s Sanction Policy.

pdfelement

Remove Watermark Now

HIPAA5-Documentation Availability

Updated: 7/30/18

Introduction

CHANGES REHABILITATION LLC. has adopted this HIPAA Documentation Availability Policy in order to recognize the requirement to comply with the Health Insurance Portability and Accountability Act ("HIPAA"), as amended by the Health Information Technology for Economic and Clinical Health ("HITECH") Act of 2009 (Title XIII of division A and Title IV of division B of the American Recovery and Reinvestment Act "ARRA") and the HIPAA Omnibus Final Rule (Effective Date: March 26, 2013). We acknowledge that full compliance with the HIPAA Final Rule is required by or before September 23, 2013.

CHANGES REHABILITATION LLC. hereby acknowledges our duty and responsibility to protect the privacy and security of Individually Identifiable Health Information ("IIHI") generally, and Protected Health Information ("PHI") as defined in the HIPAA Regulations, under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under principles of general and professional ethics. We also acknowledge our duty and responsibility to support and facilitate the timely and unimpeded flow of health information for lawful and appropriate purposes.

Scope of Policy

This policy governs HIPAA Documentation Availability for **CHANGES REHABILITATION LLC.**All personnel of **CHANGES REHABILITATION LLC.**must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

pdfelement

Assumptions

- **CHANGES REHABILITATION LLC.** must comply with HIPAA and the HIPAA implementing regulations concerned with the availability of HIPAA-related documentation, in accordance with the HIPAA requirements at § 164.310, § 164.316, and § 164.530(j), among others.
- **CHANGES REHABILITATION LLC.** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA Regulations.
- **CHANGES REHABILITATION LLC.** must comply with HIPAA and the HIPAA implementing regulations, in accordance with the requirements at 45 CFR Parts 160 and 164, as amended.
- Full compliance with HIPAA is mandatory and failure to comply can bring severe sanctions and penalties. Possible sanctions and penalties include, but are not limited to: civil monetary penalties, criminal penalties including prison sentences, and loss of revenue and reputation from negative publicity.
- Full compliance with HIPAA strengthens our ability to meet other compliance obligations, and will support and strengthen our non-HIPAA compliance requirements and efforts.
- Full compliance with HIPAA reduces the overall risk of inappropriate uses and disclosures of Protected Health Information (PHI), and reduces the risk of breaches of confidential health data.
- The requirements of the HIPAA Administrative Simplification Regulations (including the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules) implement sections 1171-1180 of the Social Security Act (the Act), sections 262 and 264 of Public Law 104-191, section 105 of 492 Public Law 110-233, sections 13400-13424 of Public Law 111-5, and section 1104 of Public Law 111-148.
- Entities subject to HIPAA Rules are also subject to other federal statutes and regulations. For example, federal programs must comply with the statutes and regulations that govern them. Pursuant to their contracts, Medicare providers must comply with the requirements of the Privacy Act of 1974. Substance abuse treatment facilities are subject to the Substance Abuse Confidentiality provisions of the Public Health Service Act, section 543 and its regulations. And, health care providers in schools, colleges, and universities may come within the purview of the Family Educational Rights and Privacy Act.

Policy Statement

Remove Watermark Now

- It is the Policy of **CHANGES REHABILITATION LLC.**to make all HIPAA-related documentation available to those persons responsible for implementing the policies and/or procedures to which such documentation pertains.
- All HIPAA-related documentation shall be distributed or made otherwise available to all workforce members who are affected by the documentation, or who require such documentation in the performance of their work-related duties.
- Workforce members affected by specific HIPAA-related documentation shall have access to such documentation prior to their beginning or executing work that depends on such documentation.
- No member of the workforce shall be held accountable for compliance with any HIPAA-related documentation, policies, or procedures unless they have been given access to such documentation.

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **CHANGES REHABILITAION LLC.**'s Sanction Policy.

pdfelement

Remove Watermark Now

HIPAA6-Documentation Update

Updated: 7/30/18

Introduction

CHANGES REHABILITATION has adopted this HIPAA Documentation Updating Policy in order to recognize the requirement to comply with the Health Insurance Portability and Accountability Act ("HIPAA"), as amended by the Health Information Technology for Economic and Clinical Health ("HITECH") Act of 2009 (Title XIII of division A and Title IV of division B of the American Recovery and Reinvestment Act "ARRA") and the HIPAA Omnibus Final Rule (Effective Date: March 26, 2013). We acknowledge that full compliance with the HIPAA Final Rule is required by or before September 23, 2013.

CHANGES REHABILITATION hereby acknowledges our duty and responsibility to protect the privacy and security of Individually Identifiable Health Information ("IIHI") generally, and Protected Health Information ("PHI") as defined in the HIPAA Regulations, under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under principles of general and professional ethics. We also acknowledge our duty and responsibility to support and facilitate the timely and unimpeded flow of health information for lawful and appropriate purposes.

Scope of Policy

This policy governs HIPAA Documentation Updating for **CHANGES REHABILITATION**. All personnel of **CHANGES REHABILITATION** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

pdfelement

Assumptions

- **CHANGES REHABILITATION** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA Regulations.
- **CHANGES REHABILITATION** must comply with HIPAA and the HIPAA implementing regulations, in accordance with the requirements at 45 CFR Parts 160 and 164, as amended.
- Full compliance with HIPAA is mandatory and failure to comply can bring severe sanctions and penalties. Possible sanctions and penalties include, but are not limited to: civil monetary penalties, criminal penalties including prison sentences, and loss of revenue and reputation from negative publicity.
- Full compliance with HIPAA strengthens our ability to meet other compliance obligations, and will support and strengthen our non-HIPAA compliance requirements and efforts.
- Full compliance with HIPAA reduces the overall risk of inappropriate uses and disclosures of Protected Health Information (PHI), and reduces the risk of breaches of confidential health data.
- The requirements of the HIPAA Administrative Simplification Regulations (including the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules) implement sections 1171-1180 of the Social Security Act (the Act), sections 262 and 264 of Public Law 104-191, section 105 of 492 Public Law 110-233, sections 13400-13424 of Public Law 111-5, and section 1104 of Public Law 111-148.
- Entities subject to HIPAA Rules are also subject to other federal statutes and regulations. For example, federal programs must comply with the statutes and regulations that govern them. Pursuant to their contracts, Medicare providers must comply with the requirements of the Privacy Act of 1974. Substance abuse treatment facilities are subject to the Substance Abuse Confidentiality provisions of the Public Health Service Act, section 543 and its regulations. And, health care providers in schools, colleges, and universities may come within the purview of the Family Educational Rights and Privacy Act.

Policy Statement

Remove Watermark Now

- It is the Policy of **CHANGES REHABILITATION** to review all HIPAA-related documentation periodically, and update such documentation as needed, in response to environmental or operation changes affecting the privacy or security of individually identifiable health information.
- Reviews of HIPAA-related documentation shall be made periodically, but at least every 12 months for the purposes of this policy.
- Reviews and updates of HIPAA-related documentation that occur as a result of this policy shall be made by **CHANGES REHABILITATION**'s designated Corporate Compliance Officer.
- Reviews and updates of HIPAA-related documentation that occur as a result of this policy shall be documented according to **CHANGES REHABILITATION**'s Documentation Policy.

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **CHANGES REHABILITATION**'s Sanction Policy.

pdfelement

Remove Watermark Now

HIPAA7-Investigations Policy
Updated: 7/30/18

Introduction

CHANGES REHABILITATION LLC. has adopted this HIPAA Investigations Policy in order to recognize the requirement to comply with the Health Insurance Portability and Accountability Act ("HIPAA"), as amended by the Health Information Technology for Economic and Clinical Health ("HITECH") Act of 2009 (Title XIII of division A and Title IV of division B of the American Recovery and Reinvestment Act "ARRA") and the HIPAA Omnibus Final Rule (Effective Date: March 26, 2013). We acknowledge that full compliance with the HIPAA Final Rule is required by or before September 23, 2013.

CHANGES REHABILITATION LLC. hereby acknowledges our duty and responsibility to protect the privacy and security of Individually Identifiable Health Information ("IIHI") generally, and Protected Health Information ("PHI") as defined in the HIPAA Regulations, under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under principles of general and professional ethics. We also acknowledge our duty and responsibility to support and facilitate the timely and unimpeded flow of health information for lawful and appropriate purposes.

Scope of Policy

This policy governs HIPAA Investigations for **CHANGES REHABILITATION LLC.** All personnel of **CHANGES REHABILITATION LLC.**must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

pdfelement

Assumptions

- **CHANGES REHABILITATION LLC.** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA Regulations.
- **CHANGES REHABILITATION LLC.** must comply with HIPAA and the HIPAA implementing regulations, in accordance with the requirements at 45 CFR Parts 160 and 164, as amended.
- Full compliance with HIPAA is mandatory and failure to comply can bring severe sanctions and penalties. Possible sanctions and penalties include, but are not limited to: civil monetary penalties, criminal penalties including prison sentences, and loss of revenue and reputation from negative publicity.
- **CHANGES REHABILITATION LLC.**recognizes that the U.S. Department of Health and Human Services ("HHS"), its Office for Civil Rights ("OCR") and other designees, as well as State Attorneys General, are all authorized and empowered to investigate Covered Entities and Business Associates in matters of HIPAA compliance and enforcement.
- **CHANGES REHABILITATION LLC.**recognizes that timely and full cooperation with such investigative bodies is mandatory under HIPAA law; and that failure to cooperate with any HIPAA investigation is itself a violation of HIPAA Rules.

Policy Statement

- It is the Policy of **CHANGES REHABILITATION LLC.**to fully comply with HIPAA law and with all HIPAA-related investigations conducted by HHS.
- It is the Policy of **CHANGES REHABILITATION LLC.**to not impede or obstruct any HIPAA-related investigations conducted by HHS.
- It is the Policy of **CHANGES REHABILITATION LLC.**to provide all documentation or assistance required by law in connection with any HIPAA-related investigations conducted by HHS.

Remove Watermark Now

Procedures

Workforce members who are designated to assist with HIPAA-related investigations conducted by HHS must adhere to the following procedures:

- Whenever a HHS investigation is discovered, the following persons must be immediately notified:
  - Corporate Office
  - Executive Management
  - Corporate Compliance Officer
  - Director of IT
- Cooperate, but do not volunteer information or records that are not requested.
- Ask for the official government agency-issued identification of the investigators (Business cards are NOT official identification); write down their names, office addresses, telephone numbers, fax numbers and e-mail addresses. If investigators cannot produce acceptable I.D., call legal counsel immediately and defer the provision of any PHI until after you confer with counsel or until the investigators produce acceptable I.D. BE SURE that you've made appropriate requests for I.D. and that they've been unreasonably refused before you do.)
- Have at least one, if not two witnesses available to testify as to your requests and their responses.
- Ask for the name and telephone number of the lead investigator's supervisor, but only if, in your judgment, his/her demeanor indicates that you can ask such a question without engendering "hard feelings." Under NO circumstances should you take any action to escalate tensions, except if you genuinely doubt the identity or authority of the investigators.
- Determine if there are any law enforcement personnel present (i.e., FBI, US Attorney investigators, State Prosecutor investigators, etc.). If law enforcement personnel are present, then the investigation is likely a criminal one, with much more severe penalties than may result from a civil investigation. Generally, guns strapped to hips are a good indicator of the presence of law enforcement personnel; but, if in doubt, ask.
- Permit the investigators to have access to protected health information ("PHI"), in accordance with our notice of privacy practices ("NPP"), and Federal and State law. Once investigators have verified their identities and have also verified their authority to access PHI, it is a violation of HIPAA to withhold PHI from them, if the PHI sought is the subject matter of the investigation, or reasonably related to the investigation. Again, ask investigators to verify that they are seeking access to the information because it is directly related to their legitimate investigatory purposes; and document their responses in your own written records.
- Have a witness with you when you ask about their authority to access PHI, and the use that they will make of the PHI they are seeking access to, who can later testify as to what they told you. Two witnesses are even better. All witnesses should also prepare a written summary of the conduct and communications they observed as soon as possible after the incident; these summaries should be annotated with the time and date of the event, the time and date that the summaries were completed, and the witnesses signature.
- Send staff employees elsewhere, if possible, during this first investigation encounter. There is no requirement that we provide witnesses to be questioned during the initial phase of an investigation.
- Do NOT instruct employees to hide or conceal facts, or otherwise mislead investigators.
- Ask the investigators for documents related to the investigation. For example, request:
  - copies of any search warrants and/or entry and inspection orders
  - copies of any complaints
  - a list of patients they are interested in
  - a list of documents/items seized
- Do NOT expect that investigators will provide any of the above, except for the search warrant and a list of documents/items seized (if any).
- Do not leave the investigators alone, if possible. Assign someone to "assist" each investigator present.
- Do not offer food (coffee, if already prepared, and water, if already available, is ok. Don't do anything that could be construed as a "bribe" or a "kickback" to induce favorable treatment, such as offering to buy the investigators lunch.
- Tell investigators what you are required by law to tell them. Answer direct questions fully and to the best of your ability. Always defer to the advice of legal counsel if you are unsure of what or how much to say.

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **CHANGES REHABILITATION LLC.**' s Sanction Policy.

pdfelement

Remove Watermark Now

HIPAA8-Breach Notification

Updated: 7/30/18

CHANGES REHABILITATION LLC. has adopted this Breach Notification Policy in order to recognize the requirement to comply with the Health Insurance Portability and Accountability Act ("HIPAA"), as amended by the Health Information Technology for Economic and Clinical Health ("HITECH") Act of 2009 (Title XIII of division A and Title IV of division B of the American Recovery and Reinvestment Act "ARRA") and the HIPAA Omnibus Final Rule (Effective Date: March 26, 2013). We acknowledge that full compliance with the HIPAA Final Rule is required by or before September 23, 2013.

CHANGES REHABILITATION LLC. hereby acknowledges our duty and responsibility to protect the privacy and security of Individually Identifiable Health Information ("IIHI") generally, and Protected Health Information ("PHI") as defined in the HIPAA Regulations, under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under principles of general and professional ethics. We also acknowledge our duty and responsibility to support and facilitate the timely and unimpeded flow of health information for lawful and appropriate purposes.

Scope of Policy

This policy governs Breach Notification for **CHANGES REHABILITATION LLC.** All personnel of **CHANGES REHABILITATION LLC.** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

pdfelement

Assumptions

- ❑ **CHANGES REHABILITATION LLC.** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
- ❑ **CHANGES REHABILITATION LLC.** must comply with HIPAA and the HIPAA implementing regulations concerned with notifications to patients and consumers about breaches of individually identifiable health information, in accordance with the requirements at § 164.400 to § 164.414.
- ❑ Compliance with HIPAA's breach notification requirements is mandatory and failure to comply can bring severe sanctions and penalties.
- ❑ Timely notifications to consumers about breaches of individually identifiable health information can help reduce or prevent identity theft and fraud.
- ❑ Timely notifications to consumers about breaches of individually identifiable health information can help protect our business and reputation.
- ❑ Only breaches of "unsecured" (unencrypted or not destroyed) protected health information trigger HIPAA's breach notification requirements.

Definitions

As used within the HIPAA Final ("Omnibus") Rule, the following terms have the following meanings:

Breach means the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information.

1. Breach excludes:
    i. Any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under subpart E of this part.

ii. Any inadvertent disclosure by a person who is authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under subpart E of this part.

iii. A disclosure of protected health information where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

2. Except as provided in paragraph (1) of this definition, an acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:

   i. The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;

   ii. The unauthorized person who used the protected health information or to whom the disclosure was made;

   iii. Whether the protected health information was actually acquired or viewed; and

   iv. The extent to which the risk to the protected health information has been mitigated.

Unsecured protected health information means protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Pub. L. 111-5.

Policy Statement

- It is the Policy of **CHANGES REHABILITATION LLC.**to provide timely notifications to affected (patients and/or) consumers about breaches of individually identifiable health information.
- Model breach notification letters or emails shall be developed and prepared to be used as needed.
- **CHANGES REHABILITAION LLC.**shall notify individuals when a reportable breach is discovered . A breach is treated as "discovered" by **CHANGES REHABILITATION LLC.** the first day on which such breach is known or should reasonably have been known to any employee or agent of **CHANGES REHABILITATION LLC.**, other than the person who committed the breach.
- Notification must occur without unreasonable delay and in no event later than 60 days from discovery of the breach, unless law enforcement requests a delay.

Procedures

- Breach Notices must include a brief description of what happened, a description of the types of PHI involved, steps the individual should take to protect themselves from potential harm, a brief description of the actions taken in response to the breach, and contact procedures for the individual to ask questions.
- First class mail shall be the default method of notification . **CHANGES REHABILITATION LLC.**may use e-mail if requested by the individual, or substitute notice via our website or local print or broadcast media if we do not have current contact information.
- **CHANGES REHABILITATION LLC.** must notify major local media outlets of a breach affecting more than 500 individuals.
- Business Associates of **CHANGES REHABILITATION LLC.** are required to immediately report all breaches, losses, or compromises of individually identifiable health information – whether secured or unsecured – to **CHANGES REHABILITATION LLC.**'s Corporate Compliance Officer.
- Business Associate contracts, whether existing or new, shall have corresponding breach notification requirements included in them.
- Sanctions or re-training shall be applied to all workforce members who caused or created the conditions that allowed the breach to occur, according to **CHANGES REHABILITATION.**'s Sanctions Policy.
- All breach-related activities and investigations shall be thoroughly and timely documented in accordance with **CHANGES REHABILITATION.**'s Documentation Policy.

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **CHANGES REHABILITATION LLC.**'s Sanctions Policy.

Remove Watermark Now
pdfelement

Remove Watermark Now

HIPAA9-Privacy-Official Policy
Updated: 7/30/18

Introduction

CHANGES REHABILITATION LLC. has adopted this Privacy-Official Policy in order to recognize the requirement to comply with the Health Insurance Portability and Accountability Act ("HIPAA"), as amended by the Health Information Technology for Economic and Clinical Health ("HITECH") Act of 2009 (Title XIII of division A and Title IV of division B of the American Recovery and Reinvestment Act "ARRA") and the HIPAA Omnibus Final Rule
(Effective Date: March 26, 2013). We acknowledge that full compliance with the HIPAA Final Rule is required by or before September 23, 2013.

CHANGES REHABILITATION LLC. hereby acknowledges our duty and responsibility to protect the privacy and security of Individually Identifiable Health Information ("IIHI") generally, and Protected Health Information ("PHI") as defined in the HIPAA Regulations, under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under principles of general and professional ethics. We also acknowledge our duty and responsibility to support and facilitate the timely and unimpeded flow of health information for lawful and appropriate purposes.

Scope of Policy

This policy governs designation of a Corporate Compliance Officer for **CHANGES REHABILITATION LLC.** All personnel of **CHANGES REHABILITATION LLC.** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

pdfelement

Assumptions

- **CHANGES REHABILITATION LLC.** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA Regulations.
- **CHANGES REHABILITATION LLC.** must comply with HIPAA and the HIPAA implementing regulations, in accordance with the requirements at 45 CFR Parts 160 and 164, as amended.
- Full compliance with HIPAA is mandatory and failure to comply can bring severe sanctions and penalties. Possible sanctions and penalties include, but are not limited to: civil monetary penalties, criminal penalties including prison sentences, and loss of revenue and reputation from negative publicity.
- **CHANGES REHABILITATION LLC.** recognizes that the designation of a Privacy Official /Corporate Compliance Officer is mandatory under the HIPAA Rules ; and that the designation of a Privacy Official/ Corporate Compliance Officer provides numerous benefits to **CHANGES REHABILITATION LLC.**

Policy Statement

- It is the Policy of **CHANGES REHABILITATION LLC.** to designate and maintain at all times an active HIPAA Privacy Official/Corporate Compliance Officer.
- The Corporate Compliance Officer for **CHANGES REHABILITATION LLC.** is:

  Dr. Shirley Jankowski

- The Corporate Compliance Officer's general responsibilities are to:
  - Oversee all HIPAA-related compliance activities, including the development, implementation and maintenance of appropriate privacy and security-related policies and procedures.
  - Conduct various risk analyses, as needed or required.
  - Manage breach notification investigations, determinations, and responses, including breach notifications.
  - Develop or obtain appropriate privacy and security training for all workforce members, as appropriate.

Remove Watermark Now

Procedures

CHANGES REHABILITATION LLC.'s Corporate Compliance Officer, and his or her designees, shall be responsible for implementing, managing, and maintaining the following procedures:

- ❑ Ensure compliance with privacy practices and consistent application of sanctions for failure to comply with privacy policies for all individuals in the organization's workforce, extended workforce, and for all business associates, in cooperation with Human Resources, Director of IT, administration, and legal counsel as applicable.
- ❑ Maintain an accurate inventory of (1) all individuals who have access to confidential information, including PHI, and (2) all uses and disclosures of confidential information by any person or entity.
- ❑ Administer patient requests under HIPAA's Patient Rights.
- ❑ Administer the process for receiving, documenting, tracking, investigating, and taking action on all complaints concerning the organization's privacy policies and procedures in coordination and collaboration with other similar functions and, when necessary, legal counsel.
- ❑ Cooperate with HHS and its Office for Civil Rights, other legal entities, and organization officers in any compliance reviews or investigations.
- ❑ Work with appropriate technical personnel to protect confidential information from unauthorized use or disclosure.
- ❑ Develop specific policies and procedures mandated by HIPAA.
- ❑ Develop additional relevant policies, such as policies governing the inclusion of confidential data in emails, and access to confidential data by telecommuters.
- ❑ Draft and disseminate the Privacy Notice required by the Privacy Rule.
- ❑ Determine when consent or authorization is required for uses or disclosures of PHI, and draft forms as necessary.
- ❑ Review all contracts under which access to confidential data is given to outside entities, bring those contracts into compliance with the Privacy Rule, and ensure that confidential data is adequately protected when such access is granted.
- ❑ Ensure that all policies, procedures and notices are flexible enough to respond to new technologies and legal requirements, or, if they are not, amend as necessary.
- ❑ Ensure that future initiatives are structured in such a way as to ensure patient privacy.
- ❑ Conduct periodic privacy audits and take remedial action as necessary.
- ❑ Oversee employee training in the areas of information privacy and security.
- ❑ Deter retaliation against individuals who seek to enforce their own privacy rights or those of others.
- ❑ Remain up-to-date and advise on new technologies to protect data privacy.
- ❑ Remain up-to-date on laws, rules and regulations regarding data privacy and update the Practice's policies and procedures as necessary.
- ❑ Track pending legislation regarding data privacy and if appropriate, seek to favorably influence that legislation.
- ❑ Anticipate patient or consumer concerns about our use of their confidential information, and develop policies and procedures to respond to those concerns and questions.
- ❑ Evaluate privacy implications of online, web-based applications.
- ❑ Monitor data collected by or posted on our website(s) for privacy concerns.
- ❑ Serve as liaison to government agencies, industry groups and privacy activists in all matters relating to our privacy practices.

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **CHANGES REHABILITATION LLC.**'s Sanction Policy.

Templefolement

Remove Watermark Now

HIPAA10-State Law Preemption Policy
Updated: 7/30/18

Introduction

CHANGES REHABILITATION LLC. has adopted this HIPAA/State Law Preemption Policy in order to recognize the requirement to comply with the Health Insurance Portability and Accountability Act ("HIPAA"), as amended by the Health Information Technology for Economic and Clinical Health ("HITECH") Act of 2009 (Title XIII of division A and Title IV of division B of the American Recovery and Reinvestment Act "ARRA") and the HIPAA Omnibus Final Rule (Effective Date: March 26, 2013). We acknowledge that full compliance with the HIPAA Final Rule is required by or before September 23, 2013.

CHANGES REHABILITATION LLC. hereby acknowledges our duty and responsibility to protect the privacy and security of Individually Identifiable Health Information ("IIHI") generally, and Protected Health Information ("PHI") as defined in the HIPAA Regulations, under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under principles of general and professional ethics. We also acknowledge our duty and responsibility to support and facilitate the timely and unimpeded flow of health information for lawful and appropriate purposes.

Scope of Policy

This policy governs HIPAA Preemption and State Law for **CHANGES REHABILITATION LLC.**All personnel of **CAHNGES REHABILITATION LLC.**must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

pdfelement

Assumptions

- ❑ **CHANGES REHABILITATION LLC.** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
- ❑ **CHANGES REHABILITATION LLC.** must comply with HIPAA and the HIPAA implementing regulations concerning state law preemptions of HIPAA regulations, in accordance with the requirements at § 160.201 to § 160.205.
- ❑ HIPAA generally preempts state laws regarding medical or health privacy. However, state laws that provide stronger protections for confidential health data, or that provide for better patient and consumer access to health data than HIPAA, will generally preempt HIPAA regulations.
- ❑ HIPAA Covered Entities and Business Associates must follow both HIPAA law and state law when possible. If there is a conflict between the two, a preemption analysis and determination must be made to assess which laws (HIPAA, State Laws, or both) must be followed.

Policy Statement

- ❑ It is the Policy of **CHANGES REHALBILITATION LLC.**to comply, whenever possible, with state law in the state(s) where we operate, as well as HIPAA law and regulations.

Procedures

- ❑ **CHANGES REHABILITATION LLC.LLC.**'s designated Corporate Compliance Officer shall analyze HIPAA preemption issues, in cooperation with legal counsel, and make preemption determinations.
- ❑ **CHANGES REHABILITATION LLC..**'s designated Corporate Compliance Officer shall create, modify, or amend organization policies to accurately reflect preemption determinations and provide guidance to management on HIPAA and state law preemption issues.
- ❑ If off-the-shelf or custom preemption analyses are obtained from external sources, it is the responsibility of the **CHANGES REHABILITATION LLC..**'s designated Corporate Compliance Officer, in cooperation with legal

counsel, to certify the validity and accuracy of such external preemption analyses before applying those analyses to **CHANGES REHABILITATION LLC.LLC.** operations.

- **CHANGES REHABILITATION LLC. LLC.**'s designated Corporate Compliance Officer shall conduct ongoing research to monitor legislative changes in the state(s) where we operate that could affect HIPAA preemption issues.

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **CHANGES REHABILITATION LLC..**' s Sanction Policy.

Remove Watermark Now
pdfelement

Remove Watermark Now

HIPAA11-Training Policy
Updated: 7/30/18

Introduction

CHANGES REHABILITATION LLC.. has adopted this HIPAA Training Policy in order to recognize the requirement to comply with the Health Insurance Portability and Accountability Act ("HIPAA"), as amended by the Health Information Technology for Economic and Clinical Health ("HITECH") Act of 2009 (Title XIII of division A and Title IV of division B of the American Recovery and Reinvestment Act "ARRA") and the HIPAA Omnibus Final Rule
(Effective Date: March 26, 2013). We acknowledge that full compliance with the HIPAA Final Rule is required by or before September 23, 2013.

CHANGES REHABILITATION LLC.. hereby acknowledges our duty and responsibility to protect the privacy and security of Individually Identifiable Health Information ("IIHI") generally, and Protected Health Information (" PHI") as defined in the HIPAA Regulations, under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under principles of general and professional ethics. We also acknowledge our duty and responsibility to support and facilitate the timely and unimpeded flow of health information for lawful and appropriate purposes.

Scope of Policy

This policy governs HIPAA Privacy and Security Training for **CHANGES REHABILITATION LLC.**All personnel of **CHANGES REHABILITATION INC** must comply with this policy . Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

Assumptions

- ❑ **CHANGES REHABILITATION LLC.** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
- ❑ **CHANGES REHABILITATION LLC.** must comply with HIPAA and the HIPAA implementing regulations concerning the training of workforce members, in accordance with the requirements at § 164.530(b).
- ❑ Clear and complete HIPAA training, in combination with appropriate HIPAA awareness resources, can significantly reduce the likelihood of breaches of confidential health information and the likelihood of HIPAA violations.

Policy Statement ❑ It is the Policy of **CHANGES REHABILITATION LLC..** to provide clear and complete HIPAA training to all members of the workforce, including officers, agents, employees, contractors, temporary workers,

and volunteers.

❑ HIPAA training provided by **CHANGES REHABILITATION LLC..** shall include relevant and appropriate aspects of both health data privacy and health data security, as it pertains to **CHANGES REHABILITATION LLC.** 's operations and to the duties and responsibilities of specific individuals, workgroups, departments, and divisions.

Procedures

- ❑ HIPAA training, at minimum, shall include the basics of HIPAA itself; the basics of HIPAA's privacy and security requirements and restrictions; and a review of relevant and appropriate internal Policies and Procedures related to HIPAA and HIPAA compliance.
- ❑ HIPAA training shall be provided to all new hires during the new employee orientation period, before new employees are exposed to or work with individually identifiable health information.
- ❑ HIPAA training shall be conducted periodically for all employees, but no less than twice anually.

- ❑ Fostering ongoing, continuous HIPAA awareness shall be regarded as a separate type of workforce learning from regular HIPAA training. The designated Corporate Compliance Officer shall be responsible

for the development (or acquisition), and deployment of appropriate HIPAA awareness materials to maintain a high level of HIPAA awareness among the workforce.

- The designated Corporate Compliance Officer is responsible for the development or acquisition of appropriate HIPAA training and awareness resources.
- HIPAA training resources should aim to develop a general understanding of HIPAA and its requirements and restrictions. HIPAA awareness resources should aim to maintain a high level of HIPAA awareness, and a protective attitude toward confidential data on an ongoing, daily basis.
- Employees will use Relias to complete their ongoing HIPAA training.

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **CHANGES REHABILITATION LLC**.'s Sanction Policy.

Remove Watermark Now
pdfelement

Remove Watermark Now

HIPAA12-PHI Uses and Disclosures Policy

Updated: 7/30/18

Introduction

CHANGES REHABILITATION LLC.. has adopted this Protected Health Information ("PHI") Uses and Disclosures Policy in order to recognize the requirement to comply with the Health Insurance Portability and Accountability Act
("HIPAA"), as amended by the Health Information Technology for Economic and Clinical Health ("HITECH") Act of 2009 (Title XIII of division A and Title IV of division B of the American Recovery and Reinvestment Act "ARRA") and the HIPAA Omnibus Final Rule (Effective Date: March 26, 2013). We acknowledge that full compliance with the HIPAA Final Rule is required by or before September 23, 2013.

CHANGES REHABILITATION LLC.. hereby acknowledges our duty and responsibility to protect the privacy and security of Individually Identifiable Health Information ("IIHI") generally, and Protected Health Information (" PHI") as defined in the HIPAA Regulations, under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under principles of general and professional ethics. We also acknowledge our duty and responsibility to support and facilitate the timely and unimpeded flow of health information for lawful and appropriate purposes.

Scope of Policy

This policy governs the permitted uses and disclosures of Protected Health Information for **CHANGES REHABILITATION LLC.**All personnel of **CHANGES REHABILITATION LLC.**must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

Assumptions

- **CHANGES REHABILITATION LLC..** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
- **CHANGES REHABILITATION LLC.**must comply with HIPAA and the HIPAA implementing regulations concerning uses and disclosures of Protected Health Information, in accordance with the requirements at § 164.502 to § 164.514.
- **CHANGES REHABILITATION LLC.**must implement policies and procedures to ensure that all uses and disclosures of PHI are made or denied in accordance with HIPAA law and regulations.
- For especially sensitive information, such as AIDS/HIV, alcohol and drug abuse prevention and treatment, and the like, patient consent to disclosure must be *informed.* That is, made with the patient's or consumer's knowledge of the risks and benefits of the disclosure.
- Any disclosure of confidential patient information carries with it the potential for an unauthorized redisclosure that breaches confidentiality.
- **CHANGES REHABILITATION LLC.**incurs costs when releasing patient information (copying, postage, and so forth) and is permitted under HIPAA Regulations and under State law to charge a reasonable fee to offset those costs.

Policy Statement

- It is the Policy of **CHANGES REHABILITATION LLC.**to conduct its operations in full compliance with HIPAA's Rules governing uses and disclosures of Protected Health Information.
- **A.** will process requests for information from patient records in a timely, consistent manner as set forth in this policy.

Procedures

- ~~The following priorities and time frames shall apply to requests for disclosures of PHI:~~

pdfelement

- *Emergency requests involving immediate emergency care of patient:* immediate processing.
- *Priority requests pertaining to current care of patient:* within one workday.
- *Patient request for access to own record:* within three (3) workdays.
- *Subpoenas and depositions:* as required.
- *All other requests:* within five (5) workdays

- Courtesy Notifications to Practitioners – As a courtesy, records processing personnel shall notify the appropriate healthcare practitioner when any of the following occur:
  - Patient or his or her representative requests information from the medical record.
  - Patient or representative requests direct access to the complete medical record.
  - Patient or representative institutes legal action.
- Disclosure Monitoring and Logging -- Medical Records personnel will maintain a log to track the step-by-step process towards completion of each request for the release of PHI. Medical Records personnel will review and update this log daily to give proper priority to requests and to provide early intervention in problem situations. The log shall contain the following information:
  - Date department received the request.
  - Name of patient.
  - Name and status (patient, parent, guardian) of person making request.
  - Information released.
  - Date released.
  - Fee charged.
- Fee Schedule – **CHANGES REHABILITATION LLC.** will process requests for information from patient records in a timely, consistent manner as set forth in this policy.
- **CHANGES REHABILITATION LLC..** may charge a reasonable fee to offset the costs associated with specific categories of requests. **CHANGES REHABILITATION LLC.**shall develop and implement a Fee Schedule related to disclosures of PHI. Fees shall be based on an assessment of such factors as the costs of equipment and supplies, employee costs, and administrative overhead and shall include postage (including express mail or courier costs) when incurred at the request of the authorizing party. For requests for records in electronic format, HIPAA permits fees to include only direct labor costs when responding to such requests. Individual states have also established maximum fees for copies of patient records.
- Unless the request specifies release of the complete medical record, **CHANGES REHABILITATION INC ..** shall release only selected portions of the record. **CHANGES REHABILITATION LLC.**shall prepare an appropriate cover letter detailing the items included.
- Prohibition of Redisclosure -- Unless a law or regulation requires a more specific prohibition on redisclosure (usually for AIDS/HIV, alcohol and drug abuse, and other particularly sensitive medical information), each disclosure outside the facility shall contain the following notice:
  - *The attached medical information pertaining to [Name of patient] is confidential and legally privileged.* ***CHANGES REHABILITATION LLC.*** *has provided it to [Name of recipient] as authorized by the patient. The recipient may not further disclose the information without the express consent of the patient or as authorized by law.*
- Retention of Disclosure Requests -- The Medical Record personnel will retain the original request, the authorization for release of information, and a copy of the cover letter in the patient(s) medical record for the appropriate record retention period.
- Use of Copying Services -- To facilitate the timely processing of release of information requests, **CHANGES REHABILITATION LLC..** may use the services of a commercial copying service on terms that protect the integrity and confidentiality of patient information.
- Disclosure Quality Control -- The Medical Record personnel shall conduct a routine audit of the release of information at least quarterly, paying particular attention to the following:
  - Validity of authorizations.
  - Appropriateness of information abstracted in response to the request.
  - Retention of authorization, request, and transmitting cover letter.
  - Procedures for telephone, electronic, and in-person requests.
  - Compliance with designated priorities and time frames.
  - Proper processing of fees.
  - Maintenance of confidentiality.
- In-service Training on Disclosures – **CHANGES REHABILITATION LLC.**. shall give periodic in-service training to all employees involved in the release of information.
- Semi-Annual Policy Review – The Corporate Compliance Officer shall review this policy and associated procedures with risk management and legal counsel at least semiannually.

- Capacity to Authorize – **CHANGES REHABILITATION LLC.**requires a written, signed, current, valid authorization to release medical information as follows:

Remove Watermark Now
Buffalement

Remove Watermark Now

Patient Category	Required Signature
Adult Patient	The patient or a duly authorized representative, such as court-appointed guardian or attorney. Proof of authorized representation required (such as notarized power of attorney).
Deceased Patient	Next of kin as stated on admission face sheet (state relationship on authorization) or executor/ administrator of estate.
Unemancipated Minor	Parent, next of kin, or legally appointed guardian or attorney (proof of relationship required).
Emancipated Minor	Same as adult patients above.
Psychiatric, drug, alcohol program patients/clients	Same as adult patients above, but check for special requirements.
AIDS/HIV or other sexually transmitted disease patients	Same as adult patients above, but check for special requirements.

- Authorization Forms – **CHANGES REHABILITATION INC ..** shall develop and use an approved authorization form. All personnel will use this form whenever possible. All personnel shall, however, honor letters and other forms, provided they include all the required information.
- Revocation of Authorization -- A patient may revoke an authorization by providing a written statement to us. The revocation shall become effective when the facility receives it, but shall not apply to disclosures already made.
- Refusal to Honor Authorization -- Health Information Management Department personnel and/or the Corporate Compliance Officer, or others authorized to release information, will not honor a patient authorization when they have a reasonable doubt or question as to the following information:
  - Identity of the person presenting the authorization.
  - Status of the individual as the duly appointed representative of a minor, deceased, or incompetent person.
  - Legal age or status as an emancipated minor.
  - Patient capacity to understand the meaning of the authorization.
  - Authenticity of the patient(s) signature.
  - Current validity of the authorization.
  - In such situations, the employee shall refer the matter to the Corporate Compliance Officer for review and decision.
- Electronic Records -- The above requirements apply equally to electronic records. No employee shall release electronic records without complying with this policy.

pdfelement

Person and Identity Verification Table

Person to Identify	In-Person Encounter	Telephone Encounter	Request in Writing (Fax, mail, hand-delivered)
Attorney	▪ Presents with business card and photo identification (i.e. drivers license or organization ID badge) and:	▪ It would be difficult to verify identity and authority by phone. Verification in person or in writing may be required	▪ Supplies business card, photo identification (i.e. driver's license or org ID badge), letterhead. Confirmation call is required.
Facility Directory:	▪ Verify identity	▪ Verify identity	▪ Verify identity
Patient	▪ Patient provides name, address, and date of birth	▪ Patient provides name, address, and date of birth and/or social security	▪ Patient provides name, address, and date of birth and/or social security

Person to Identify	In-Person Encounter	Telephone Encounter	Request in Writing (Fax, mail, hand-delivered)
	and/or social security number; or ▪ Acquainted with patient	number; or ▪ Acquainted with patient	number. Verify patient's signature with that on file or on driver's license.
Personal Representative (Legal Guardian) for the Patient	▪ Personal Rep provides patient's name, address, and date of birth and/or social security number, **and** verifies (via legal docs) relationship to patient; or, ▪ Acquainted with personal Rep as such.	▪ Personal Rep provides patient's name, address, and date of birth and/or social security number, **and** verifies (via legal docs) relationship to patient; or, ▪ Acquainted with Personal Rep as such.	▪ Personal Rep provides patient's name, address, and date of birth and/or social security number. Verify the Personal Rep's signature with signature on file or on driver's license.
Persons Involved in the Patient's Immediate Care *(PHI relevant only to the patient's current care (164.510(b)).* ▪ Blood Relative ▪ Spouse ▪ Domestic Partner ▪ Roommate ▪ Boy/Girl Friend ▪ Neighbor ▪ Colleague	▪ Patient actively involves this person in his/her care; or ▪ In your best professional judgment, the disclosure is in the patient's best interest.	▪ Patient actively involves this person in his/her care; or ▪ In your best professional judgment, the disclosure is in the patient's best interest. ▪ Use call-back.	▪ N/A
Power of Attorney For the Patient	▪ Presents with a photo ID and a copy of the POA. Verify patient's signature with one on file. ▪ Acquainted with power of attorney as being such	▪ Previously obtained a copy of the POA and verified the patient's signature with one on file. ▪ Acquainted with power of attorney as being such	▪ Obtain a copy of the POA and verify the patient's signature with one on file
Provider From Another Facility	▪ Acquainted with provider as a treatment	▪ Acquainted with provider as a treatment provider;	▪ Recognize name of facility and address on letterhead as a

Remove Watermark Now
pdfelement

Person to Identify	In-Person Encounter	Telephone Encounter	Request in Writing (Fax, mail, hand-delivered)
	provider; ▪ Provider is wearing a photo badge from his/her facility; or, ▪ Patient/personal representative introduces provider to you.	or; ▪ Call requestor back through main switchboard number (not via a direct number).	treatment facility; or ▪ Call requestor back through main switchboard number (not via a direct number).
Public Official ▪ CIA ▪ Court Order ▪ FBI ▪ Law Enforcement Officer ▪ OCR ▪ OIG ▪ Public Health Agency Official ▪ Other	▪ Presents an agency I.D. badge; ▪ Presents with a written statement of legal authority; ▪ Presents with a written statement of appointment on approp. govt. letterhead; ▪ Presents with warrant, court order, or legal process issued by a grand jury, or a judicial or admin. tribunal; ▪ Presents with a contract for services or purchase order; or, ▪ Official states release is necessary to prevent or lessen the threat to the health/safety of a person/public.	▪ Official states release is necessary to prevent or lessen the threat to the health/safety of a person/public.	▪ Written statement of legal authority; ▪ Written statement of appointment on appropriate government; ▪ Warrant, court order, or other legal process issued by a grand jury or a judicial or administrative tribunal; or ▪ Contract for services or purchase order
Vendor Who Helps Assists w Treatment, Payment, or Health Care Operations Examples Include, But Are Not Limited to the	▪ Recognize requestor/ organization; or ▪ Photo identification with organization	▪ Recognize requestor or organization	▪ Recognize requestor/ organization; or ▪ Call requestor back through main switchboard number (not via a direct number).

Remove Watermark Now
pdfelement

Person to Identify	In-Person Encounter	Telephone Encounter	Request in Writing (Fax, mail, hand-delivered)
Following: ▪ Accreditation Org. ▪ DME Company ▪ Insurance Co. ▪ Pharmacy Vendor we have rebate agreement with ▪ Software Vendor ▪ Statement Vendor			
1. **Workforce Member of Our Organization**	▪ Acquainted with individual as a workforce member; or, ▪ Workforce member is wearing an I.D. badge.	▪ Acquainted with individual as a workforce member; or, ▪ Workforce member is calling from an in-house extension.	▪ Request is sent from/through our own computer system; or ▪ Request is on our own letterhead.

Remove Watermark Now
pdfelement

PHI Disclosures Table

Requestor	Authorization Required?	Copy Fee Charged?	Track on Disclosure Accounting?
Accrediting Agencies (JCAHO, CARF)	No	No	No
Attorney for Resident	Yes	Yes	No
Attorney for Facility/Corporation	No	No	No
Contractors/ Business Associates	No, unless their purpose falls outside of TPO.	No	No
For Deceased Persons ❑ Coroner or Medical Examiner, Funeral Directors ❑ Organ Procurement	No	No	Yes
Employer ❑ PHI specific to work related illness or injury, and ❑ Required for employer's compliance with occupational safety and health laws	No, for the purpose listed. Yes for all others.	No	No
Family Members	No for oral disclosures to family members involved in care; Yes for others.	Yes	No

Requestor	Authorization Required?	Copy Fee Charged?	Track on Disclosure Accounting?
Entity Subject to the Food and Drug Administration ❑ Adverse events, product defects or biological product deviations ❑ Track products ❑ Enable product recalls, repairs, or replacements ❑ Conduct post marketing surveillance	No	No	Yes
Health Oversight ❑ Government benefits program ❑ Fraud and abuse compliance ❑ Civil rights laws ❑ Trauma/tumor registries ❑ Vital statistics ❑ Reporting of abuse or neglect	No	No	Yes
Health Care Practitioners and Providers for Continuity of Treatment and Payment	No	No	No
Health Care Practitioners and Providers if not Involved in Care or Treatment (i.e., consultants)	No	No	No
Insurance Companies/Third Party Payors ❑ Related to Claims Processing	No	No	No
Judicial and Administrative Proceedings ❑ Court order, or warrant ❑ Subpoena	No No - See Subpoena Policy	No Yes	Yes Yes
Law Enforcement ❑ Administrative request ❑ Locating a suspect, fugitive, material witness or missing person ❑ Victims of crime ❑ Crimes on premises ❑ Suspicious deaths ❑ Avert a serious threat to health or safety	No	No	Yes, except for disclosures to correctional institutions.
Public Health Authorities ❑ Surveillance ❑ Investigations ❑ Interventions ❑ Foreign governments collaborating with US public health authorities ❑ Recording births/deaths ❑ Child/elder abuse ❑ Prevent serious harm ❑ Communicable disease	No	No	Yes

Remove Watermark Now
pdfelement

Remove Watermark Now

Requestor	Authorization Required?	Copy Fee Charged?	Track on Disclosure Accounting?
Research (w/o Authorization)	No, if IRB or Privacy Board approves research study and waives authorization.	No	Yes
Resident/Resident's Personal Representative	No	Yes	No
Specialized Government Functions ❑ Military and Veterans' activities ❑ Protective services for the President ❑ Foreign military personnel ❑ National security and intelligence activities	No	No	Yes, except for disclosures for national security and intelligence activities.
Workers' Compensation ❑ Comply w/existing laws (see state law)	No	See applicable State Law	Yes

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **ATRIUM CENTERS LLC.**'s Sanction Policy.

pdfelement

Remove Watermark Now

HIPAA13-Patient Rights Policy
Updated: 7/30/18

Introduction

CHANGES REHABILITATION LLC. has adopted this Patient Rights Policy in order to recognize the requirement to comply with the Health Insurance Portability and Accountability Act ("HIPAA"), as amended by the Health Information Technology for Economic and Clinical Health ("HITECH") Act of 2009 (Title XIII of division A and Title IV of division B of the American Recovery and Reinvestment Act "ARRA") and the HIPAA Omnibus Final Rule
(Effective Date: March 26, 2013). We acknowledge that full compliance with the HIPAA Final Rule is required by or before September 23, 2013.

CHANGES REHABILITATION LLC. hereby acknowledges our duty and responsibility to protect the privacy and security of Individually Identifiable Health Information ("IIHI") generally, and Protected Health Information ("PHI") as defined in the HIPAA Regulations, under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under principles of general and professional ethics. We also acknowledge our duty and responsibility to support and facilitate the timely and unimpeded flow of health information for lawful and appropriate purposes.

Scope of Policy

This policy governs the provision and management of Patient Rights for **CHANGES REHABILITATION LLC.**All personnel of **CHANGES REHABILITATION LLC..** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

pdfelement

Assumptions

- **CHANGES REHABILITATION LLC..** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
- **CHANGES REHABILITATION LLC.** must comply with HIPAA and the HIPAA implementing regulations, in accordance with the requirements pertaining to the rights of patients at § 164.520, to § 164.528, as amended by the HITECH Act of 2009 (ARRA Title XIII), and the HIPAA Omnibus Final Rule (Effective Date: March 26, 2013).
- Patient information related to patient rights includes only that information contained in each patient's Designated Record Set ("DRS"), which is defined in the HIPAA regulations at § 164.501 as:
  - A group of records maintained by or for a covered entity that is:
    - The medical records and billing records about individuals maintained by or for a covered health care provider;
    - The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or
    - Used, in whole or in part, by or for the covered entity to make decisions about individuals.
  - The term "record" means any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for a covered entity.
- The provision of patient rights in a timely and positive manner can enhance the quality of care we provide to patients, by providing certain rights and controls to patients over their individually identifiable health information.

Policy Statement

- It is the Policy of **CHANGES REHABILITATION LLC.**to provide all the patient rights to our patients that are called for in the HIPAA regulations.
- Patient Rights that we provide and support include:

Remove Watermark Now

1. The Right to receive a copy of our “Notice of Privacy Practices”, which details how individually identifiable health information may be used or disclosed by this organization.
2. The Right to review or obtain a copy of medical records about that patient, or about the patient’s minor children.
3. The Right to request restrictions on the use or disclosure of the patient’s medical records.
4. The Right to receive individually identifiable health information at an alternate address or through alternate delivery means, such as by fax or courier.
5. The Right to request amendments to medical records, with certain limitations.
6. The Right to an accounting of certain disclosures of individually identifiable health information.
7. The Right to file a privacy complaint directly with us, or with the federal government.

- ❑ No retaliation of any kind is permitted against any person, patient, or workforce member for exercising any Right guaranteed by HIPAA.
- ❑ It is the Policy of **CHANGES REHABILITATION LLC..** that our Designated Record Set, for purposes of fulfilling HIPAA Patient Rights *includes* the following types or categories of data and items:
  - o Patient Medical and Billing records
  - o Records used in whole or in part by or for the provider to make clinical decisions about patients.

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **CHANGES REHABILITATION LLC..**’ s Sanction Policy.

pdfelement

Remove Watermark Now

HIPAA14-Privacy Complaints Policy
Updated: 7/30/18

Introduction

CHANGES REHABILITATION LLC. has adopted this Privacy Complaints Policy in order to recognize the requirement to comply with the Health Insurance Portability and Accountability Act ("HIPAA"), as amended by the Health Information Technology for Economic and Clinical Health ("HITECH") Act of 2009 (Title XIII of division A and Title IV of division B of the American Recovery and Reinvestment Act "ARRA") and the HIPAA Omnibus Final Rule (Effective Date: March 26, 2013). We acknowledge that full compliance with the HIPAA Final Rule is required by or before September 23, 2013.

CHANGES REHABILITATION LLC.hereby acknowledges our duty and responsibility to protect the privacy and security of Individually Identifiable Health Information ("IIHI") generally, and Protected Health Information ("PHI") as defined in the HIPAA Regulations, under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under principles of general and professional ethics. We also acknowledge our duty and responsibility to support and facilitate the timely and unimpeded flow of health information for lawful and appropriate purposes.

Scope of Policy

This policy governs the privacy complaints process for **CHANGES REHABILITATION LLC.** All personnel of **CHANGES REHABILITATION LLC.**must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

pdfelement

Assumptions

- **CHANGES REHABILITATION LLC.** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
- **CHANGES REHABILITATION LLC.** must comply with HIPAA and the HIPAA implementing regulations pertaining to privacy complaints in accordance with the requirements at § 164.530(a) and § 164.530(d), as amended by the HITECH Act of 2009 (ARRA Title XIII), and the HIPAA Omnibus Final Rule (Effective Date: March 26, 2013).
- HIPAA regulations, at § 164.530(g), prohibit intimidating or retaliatory acts against any person or patient who files a privacy complaint or exercises any Right guaranteed under HIPAA.

Policy Statement

- It is the Policy of **CHANGES REHABILITATION LLC.**to respond in a timely and positive manner to all complaints submitted by any persons or parties, including patients, workforce members, and any other person or party.
- Responsibility for the acceptance of, management of, and responses to complaints shall reside with the Corporate Compliance Officer, who shall establish a process and appropriate forms to receive and process complaints.

Procedures

- All complaints must be submitted in written form, dated and signed by the complainant.
- In addition to written complaints, anyone may call the ASAP line provided by **CHANGES REHABILITATION LLC.** to file a complaint or concern.
- **CHANGES REHABILITATION LLC..** shall investigate and respond to all complaints with a written response within 30 days of the time each complaint is submitted in writing . If more time is required to investigate and resolve a specific complaint , the complainant shall be notified in writing within 30 days of the time each complaint

is submitted in writing, that additional time is required to investigate and resolve the complaint. In no c shall more than 60 days elapse between the time a complaint is submitted in writing and the resolution of the complaint.

- If a complaint was filed over the phone, a phone call to the complainant will be made.
- The Corporate Compliance Officer shall investigate each and every complaint in a fair, impartial, and unbiased manner. All parties named in the complaint, or who participated in events leading to the complaint, shall be interviewed in a non-threatening and non-coercive manner.
- The final resolution or disposition of each complaint shall be documented in accordance with **CHANGES REHABILITATION LLC..**'s Documentation Policy, and shall be retained in accordance with **CHANGES REHABILITATION LLC.**'s Documentation Retention Policy.
- The final resolution or disposition of each complaint shall be documented and a summary of the findings shall be provided to the complainant within 30 days of the time each complaint is submitted in writing, unless the additional 30-days of response time is invoked, as above.
- In addition to providing complainants with a written response to their complaint, complaints that are found to have merit will be resolved with some remediation that is appropriate to the severity of the situation. Such remediations may include, but are not limited to:
    - A written apology to the complainant from our organization.
    - Credit-monitoring service for the complainant for a period of one or two years, paid for by our organization, when the complaint involves a breach of unsecured individually identifiable health information that has been compromised or put at risk by our actions.
    - Financial compensation, if determined to be appropriate by legal counsel and senior management.
    - Sanctions against workforce members, as appropriate to the circumstances.
    - Other unspecified remediation(s), as determined by legal counsel and senior management.
- For complaints submitted to the federal government, it is the Policy of **CHANGES REHABILITATION LLC.**to cooperate fully and openly with federal authorities as they conduct their investigation, as specified in **CHANGES REHABILITATION LLC..**'s HHS Investigations Policy.
- No officer, agent, employee, contractor, temporary worker, or volunteer of **CHANGES REHABILITATION LLC.**shall obstruct or impede any investigation in any way, whether internal or federal.

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **CHANGES REHABILITATION LLC.**' s Sanction Policy.

Remove Watermark Now
pdfelement

Remove Watermark Now

HIPAA15-Risk Management Process Policy
Updated: 7/30/18

Introduction

CHANGES REHABILITATION LLC. has adopted this Risk Management Process Policy in order to recognize the requirement to comply with the Health Insurance Portability and Accountability Act ("HIPAA"), as amended by the Health Information Technology for Economic and Clinical Health ("HITECH") Act of 2009 (Title XIII of division A and Title IV of division B of the American Recovery and Reinvestment Act "ARRA") and the HIPAA Omnibus Final Rule (Effective Date: March 26, 2013). We acknowledge that full compliance with the HIPAA Final Rule is required by or before September 23, 2013.

CHANGES REHABILITATION LLC.hereby acknowledges our duty and responsibility to protect the privacy and security of Individually Identifiable Health Information ("IIHI") generally, and Protected Health Information ("PHI") as defined in the HIPAA Regulations, under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under principles of general and professional ethics. We also acknowledge our duty and responsibility to support and facilitate the timely and unimpeded flow of health information for lawful and appropriate purposes.

Scope of Policy

This policy governs the establishment and maintenance of a Risk Management Process for **CHANGES REHABILITATION LLC.**All personnel of **CHANGES REHABILITATION LLC..** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

pdfelement

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

Assumptions

- **CHANGES REHABILITATION LLC.** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
- **CHANGES REHABILITATION LLC.**must comply with HIPAA and the HIPAA implementing regulations pertaining to the establishment and management of an appropriate risk management process , in accordance with the requirements at § 164.302 to § 164.318.
- Full compliance with HIPAA is mandatory and failure to comply can bring severe sanctions and penalties. Possible sanctions and penalties include, but are not limited to: civil monetary penalties, criminal penalties including prison sentences, and loss of revenue and reputation from negative publicity.
- The establishment and maintenance of an appropriate risk management process will generally reduce our privacy and security risk, can reduce the likelihood of creating HIPAA violations, whether inadvertent or intentional.

Policy Statement

Officers, agents, employees, contractors, temporary workers, and volunteers must read, understand, and comply with this policy.

- It is the Policy of **CHANGES REHABILITATION LLC..** to establish, implement, and maintain an appropriate risk management process.
- Such a risk management process shall be under the direct control and supervision of the Corporate Compliance Officer, and shall involve legal counsel, information technology, records management, senior management, and any other parties or persons deemed to be appropriate to the process.
- Business and information-technology "best practices", along with the research and recommendations of the National Institute for Standards and Technology ("NIST"), shall be included in the development and execution of the risk management process.

- Our risk management process shall strive to identify, analyze, prioritize, and minimize identified risks to information privacy, security, integrity, and availability. The nature and severity of various risk and risk elements shall be identified and quantified, with the goal of reducing risk as much as is practicable. The risk management process shall be ongoing, and shall be updated, analyzed, and improved on a continuous basis.
- The results of the risk management process shall be input into management's decision-making processes, in order to help reduce our overall risk and to comply with HIPAA and other applicable laws and regulations.

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **CHANGES REHABILITATION LLC.**' s Sanction Policy.

Remove Watermark Now
pdfelement

Remove Watermark Now

HIPAA16-Risk Analysis Policy
Updated: 7/30/18

Introduction

CHANGES REHABILITATION LLC.. has adopted this Risk Analysis Policy in order to recognize the requirement to comply with the Health Insurance Portability and Accountability Act ("HIPAA"), as amended by the Health Information Technology for Economic and Clinical Health ("HITECH") Act of 2009 (Title XIII of division A and Title IV of division B of the American Recovery and Reinvestment Act "ARRA") and the HIPAA Omnibus Final Rule
(Effective Date: March 26, 2013). We acknowledge that full compliance with the HIPAA Final Rule is required by or before September 23, 2013.

CHANGES REHABILITATION LLC.. hereby acknowledges our duty and responsibility to protect the privacy and security of Individually Identifiable Health Information ("IIHI") generally, and Protected Health Information (" PHI") as defined in the HIPAA Regulations, under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under principles of general and professional ethics. We also acknowledge our duty and responsibility to support and facilitate the timely and unimpeded flow of health information for lawful and appropriate purposes.

Scope of Policy

This policy governs Risk Analysis for **CHANGES REHABILITATION INC.** All personnel of **CHANGES REHABILITATION LLC.**must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

Assumptions

- **CHANGES REHABILITATION LLC.**hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
- **CHANGES REHABILITATION LLC..** must comply with HIPAA and the HIPAA implementing regulations pertaining to risk analysis, in accordance with the requirements at § 164.308(a)(1).
- Risk analysis is an integral part of this organization's overall Risk Management Process Policy and process.

Policy Statement

- It is the Policy of **CHANGES REHABILITATION LLC..** to conduct periodic assessments of potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic Protected Health Information ("ePHI") that we are entrusted with.
- Responsibility for conducting periodic risk analyses shall be with the Corporate Compliance Officer, who shall establish a plan and procedures for the conduct of such analyses.

Procedures

- All such risk analyses and assessments shall be conducted periodically, but at least annually.
- The risk analysis process shall be modeled upon the risk analysis process recommended by the National Institute for Standards and Technology ("NIST").
- The results of risk analyses and assessments shall become an integral part of management's decision-making process, and shall guide decisions related to the protection of Protected Health Information
- All such risk analyses and assessments shall be documented in accordance with this organization's Documentation Policy and HIPAA Regulations.

pdfelement

Compliance and Enforcement

Remove Watermark Now

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **CHANGES REHABILITATION LLC.**'s Sanction Policy.

pdfelement

Remove Watermark Now

HIPAA17-Risk Management Implementation Policy
Updated: 7/30/18

Introduction

CHANGES REHABILITATION LLC. has adopted this Risk Management Policy in order to recognize the requirement to comply with the Health Insurance Portability and Accountability Act ("HIPAA"), as amended by the Health Information Technology for Economic and Clinical Health ("HITECH") Act of 2009 (Title XIII of division A and Title IV of division B of the American Recovery and Reinvestment Act "ARRA") and the HIPAA Omnibus Final Rule (Effective Date: March 26, 2013). We acknowledge that full compliance with the HIPAA Final Rule is required by or before September 23, 2013.

CHANGES REHABILITATION LLC.. hereby acknowledges our duty and responsibility to protect the privacy and security of Individually Identifiable Health Information ("IIHI") generally, and Protected Health Information (" PHI") as defined in the HIPAA Regulations, under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under principles of general and professional ethics. We also acknowledge our duty and responsibility to support and facilitate the timely and unimpeded flow of health information for lawful and appropriate purposes.

Scope of Policy

This policy governs Risk Management Implementation for **CHANGES REHABILITATION LLC.**All personnel of **CHANGES REHABILITATION LLC..** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

pdfelement

Assumptions

- **CHANGES REHABILITATION LLC.** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
  - **CHANGES REHABILITATION LLC..** must comply with HIPAA and the HIPAA implementing regulations pertaining to risk management implementation, in accordance with the requirements at § 164.308(a)(1).
- Compliance with HIPAA is mandatory and failure to comply can bring severe sanctions and penalties.
- This Risk Management Implementation Policy shall be considered an integral part of our other Risk Management policies, including, but not limited to, our Risk Management Process Policy, and our Risk Analysis Policy

Policy Statement

- It is the Policy of **CHANGES REHABILITATION LLC.**to fully and completely implement our risk management process and all related policies.
- The implementation of our risk management process, analyses, and improvements shall be under the direct supervision of the designated Corporate Compliance Officer.
- The designated Corporate Compliance Officer shall develop and implement a plan, procedures, and a timetable for the implementation of our risk management process in all its aspects. Such actions shall be consistent with our other risk management policies.

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **CHANGES REHABILITATION LLC.**'s Sanctions Policy.

Remove Watermark Now

HIPAA18-Sanction Policy
Updated 7/30/18

Introduction

CHANGES REHABILITATION LLC. has adopted this Sanction Policy in order to recognize the requirement to comply with the Health Insurance Portability and Accountability Act ("HIPAA"), as amended by the Health Information Technology for Economic and Clinical Health ("HITECH") Act of 2009 (Title XIII of division A and Title IV of division B of the American Recovery and Reinvestment Act "ARRA") and the HIPAA Omnibus Final Rule
(Effective Date: March 26, 2013). We acknowledge that full compliance with the HIPAA Final Rule is required by or before September 23, 2013.

CHANGES REHABILITATION LLC. hereby acknowledges our duty and responsibility to protect the privacy and security of Individually Identifiable Health Information ("IIHI") generally, and Protected Health Information ("PHI") as defined in the HIPAA Regulations, under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under principles of general and professional ethics. We also acknowledge our duty and responsibility to support and facilitate the timely and unimpeded flow of health information for lawful and appropriate purposes.

Scope of Policy

This policy governs Workforce Sanctions and disciplinary actions for **CHANGES REHABILITATION LLC.** All personnel of **CHANGES REHABILITATION LLC..** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

pdfelement

Assumptions

- **CHANGES REHABILITATION LLC.** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
- **CHANGES REHABILITATION LLC.** must comply with HIPAA and the HIPAA implementing regulations pertaining to workforce-member sanctions, in accordance with the requirements at § 164.308(a)(1).
- Appropriate, fair and consistent sanctions have a deterrent influence on workforce transgressions; can help prevent breaches of individually identifiable health information and Protected Health Information, and can help prevent, or reduce the severity, of HIPAA violations.

Policy Statement

- It is the Policy of **CHANGES REHABILITATION LLC.**to establish and implement appropriate , fair and consistent sanctions for workforce members who fail to follow established policies and procedures, or who commit various offenses.
- Sanctions applied shall be appropriate to the nature and severity of the error or offense, and shall consist of an escalating scale of sanctions, with less severe sanctions applied to less severe errors and offenses, and more severe sanctions applied to more severe errors and offenses.
- Certain offenses can invoke immediate termination, including, but not limited to:
  - Theft
  - Intentional lying or deception
  - Drug or alcohol use while on the job
  - Violence against persons or property
- Offenses involving obvious illegal activity may result in notifications to appropriate law enforcement authorities.
- It is the Policy of **CHANGES REHABILITATION LLC..** to fully document all workforce sanctions and their dispositions, according to our Documentation Policy and HIPAA requirements.

Compliance and Enforcement

Remove Watermark Now

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **CHANGES REHABILITATION LLC..**' s Sanction Policy.

pdfelement

Remove Watermark Now

HIPAA19-Information Systems Activity Review Policy
Updated: 7/30/18

Introduction

CHANGES REHABILITATION LLC. has adopted this Information Systems Activity Review Policy in order to recognize the requirement to comply with the Health Insurance Portability and Accountability Act ("HIPAA"), as amended by the Health Information Technology for Economic and Clinical Health ("HITECH") Act of 2009 (Title XIII of division A and Title IV of division B of the American Recovery and Reinvestment Act "ARRA") and the HIPAA Omnibus Final Rule (Effective Date: March 26, 2013). We acknowledge that full compliance with the HIPAA Final Rule is required by or before September 23, 2013.

CHANGES REHABILITATION LLC. hereby acknowledges our duty and responsibility to protect the privacy and security of Individually Identifiable Health Information ("IIHI") generally, and Protected Health Information ("PHI") as defined in the HIPAA Regulations, under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under principles of general and professional ethics. We also acknowledge our duty and responsibility to support and facilitate the timely and unimpeded flow of health information for lawful and appropriate purposes.

Scope of Policy

This policy governs Information Systems Activity Reviews for **CHANGES REHABILITATION LLC.**All personnel of **CHANGES REHABILITATION INC ..** must comply with this policy . Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

pdfelement

Assumptions

- **CHANGES REHABILITATION LLC.**hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
- **CHANGES REHABILITATION LLC.** must comply with HIPAA and the HIPAA implementing regulations pertaining to information systems activity review, in accordance with the requirements at § 164.308(a)(1).

Policy Statement

- It is the Policy of **CHANGES REHABILITATION LLC.**to regularly review various indicators and records of information system activity, including, but not limited to: audit logs; access reports; and security incident reports.
- The goal of this Information Systems Activity Review Policy is to prevent, detect, contain, and correct security violations and threats to individually identifiable health information, whether in electronic or any other forms.
- It is the Policy of **CHANGES REHABILITATION LLC..** to fully document all information system activity review activities and efforts.
- This Information Systems Activity Review Policy shall be implemented and executed in accordance with our risk management policies and procedures.

Procedures

- See Information Technology Procedures IT02, IT03, IT06 and IT07.
- Annual audit.
- Corporate Compliance audit.

Compliance and Enforcement

Remove Watermark Now

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **CHANGES REHABILITATION LLC.**'s Sanction Policy.

pdfelement

Remove Watermark Now

HIPAA20-Assignment of Security Responsibility Policy
Updated: 7/30/18

Introduction

CHANGES REHABILITATION LLC. has adopted this Assignment of Security Responsibility Policy in order to recognize the requirement to comply with the Health Insurance Portability and Accountability Act ("HIPAA"), as amended by the Health Information Technology for Economic and Clinical Health ("HITECH") Act of 2009 (Title XIII of division A and Title IV of division B of the American Recovery and Reinvestment Act "ARRA") and the HIPAA Omnibus Final Rule (Effective Date: March 26, 2013). We acknowledge that full compliance with the HIPAA Final Rule is required by or before September 23, 2013.

CHANGES REHABILITATION LLC.hereby acknowledges our duty and responsibility to protect the privacy and security of Individually Identifiable Health Information ("IIHI") generally, and Protected Health Information ("PHI") as defined in the HIPAA Regulations, under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under principles of general and professional ethics. We also acknowledge our duty and responsibility to support and facilitate the timely and unimpeded flow of health information for lawful and appropriate purposes.

Scope of Policy

This policy governs the Assignment of Responsibility for health information data security for **CHANGES REHABILITATION LLC..** All personnel of **CHANGES REHABILITATION LLC.**must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

pdfelement

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

Assumptions

- **CHANGES REHABILITATION LLC..** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
- **CHANGES REHABILITATION LLC.**must comply with HIPAA and the HIPAA implementing regulations pertaining to the assignment of security responsibility, in accordance with the requirements at § 164.308 (a)(2).
- The assignment of overall security responsibility is an important and integral part of our overall risk management process, and shall be conducted in accordance and coordination with our Risk Management Process Policy.

Policy Statement

- It is the Policy of **CHANGES REHABILITATION LLC.**to assign overall responsibility for the security of individually identifiable health information , in electronic and other forms, to a person who is qualified and competent to assume such responsibility.
- The person with overall responsibility for the security of individually identifiable health information, in electronic and other forms, shall be the Corporate Compliance Officer, who shall report directly to the Board of Directors.

Procedures

The Corporate Compliance Officer shall implement the following procedures, as appropriate, in accordance with **CHANGES REHABILITATION LLC..**'s Risk Management policies:

- Ensure compliance with privacy practices and consistent application of sanctions for failure to comply with privacy policies for all individuals in the organization's workforce, extended workforce, and for all business associates, in cooperation with Human Resources, the Director of IT, administration, and legal counsel as applicable.

- ❑ Maintain an accurate inventory of (1) all individuals who have access to the Practice's confidential information, including PHI, and (2) all uses and disclosures of the Practice's confidential information by any person or entity.
- ❑ Administer patient requests and processes under HIPAA's patient rights.
- ❑ Administer the process for receiving, documenting, tracking, investigating, and taking action on all complaints concerning the organization's privacy policies and procedures in coordination and collaboration with other similar functions and, when necessary, legal counsel.
- ❑ Cooperate with the Office of Civil Rights, other legal entities, and organization officers in any compliance reviews or investigations.
- ❑ Work with appropriate technical personnel to protect the Practice's confidential information from unauthorized use or disclosure.
- ❑ Develop specific policies and procedures mandated by the Privacy Rule.
- ❑ Develop additional relevant policies, such as policies governing the inclusion of confidential data in emails, and access to confidential data by telecommuters.
- ❑ Draft and disseminate the privacy notice required by the Privacy Rule.
- ❑ Determine when the Practice might need member consent or authorization for use or disclosure of PHI, and draft forms as necessary.
- ❑ Ensure that any research efforts conducted or supported by the Practice comply with appropriate privacy laws and policies and adequately protect the privacy of the data subjects.
- ❑ Review all contracts under which access to confidential data is given to outside entities, bring those contracts into compliance with the Privacy Rule, and ensure that the Practice's confidential data is adequately protected when such access is granted.
- ❑ Ensure that all policies, procedures and notices are flexible enough to respond to new technologies and legal requirements, or, if they are not, amend as necessary.
- ❑ Ensure that future Practice initiatives are structured in such a way to ensure patient privacy.
- ❑ Conduct periodic privacy audits and take remedial action as necessary.
- ❑ Oversee employee training in the area of privacy.
- ❑ Guard against retaliation against individuals who seek to enforce their own privacy rights or those of others.
- ❑ Remain up-to-date and advise on new technologies to protect data privacy.
- ❑ Remain up-to-date on laws, rules and regulations regarding data privacy and update the Practice's policies and procedures as necessary.
- ❑ Track pending legislation regarding data privacy and if appropriate seek to influence that legislation.
- ❑ Anticipate members' concerns and questions about the Practice's use of their confidential information and develop policies and procedures to respond to those concerns and questions.
- ❑ Evaluate privacy implications of any future on-line, web-based application procedure.
- ❑ Monitor any data collected by or posted on the Practice's Web sites for privacy concerns.
- ❑ Serve as liaison to government agencies, industry groups and privacy activists in all matters relating to the Practice's privacy practices.
- ❑ It is the Policy of **CHANGES REHABILITATION LLC.** to fully document the assignment of overall security responsibility, and all related activities and efforts, according to our Documentation Policy and HIPAA requirements.

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **CHANGES REHABILITATION LLC.**'s Sanction Policy.

Remove Watermark Now
pdfelement

Remove Watermark Now

HIPAA21-Authorization and Supervision Policy
Updated: 7/30/18

Introduction

CHANGES REHABILITATION LLC.. has adopted this Authorization and Supervision Policy in order to recognize the requirement to comply with the Health Insurance Portability and Accountability Act ("HIPAA"), as amended by the Health Information Technology for Economic and Clinical Health ("HITECH") Act of 2009 (Title XIII of division A and Title IV of division B of the American Recovery and Reinvestment Act "ARRA") and the HIPAA Omnibus Final Rule (Effective Date: March 26, 2013). We acknowledge that full compliance with the HIPAA Final Rule is required by or before September 23, 2013.

CHANGES REHABILITATION LLC.. hereby acknowledges our duty and responsibility to protect the privacy and security of Individually Identifiable Health Information ("IIHI") generally, and Protected Health Information (" PHI") as defined in the HIPAA Regulations, under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under principles of general and professional ethics. We also acknowledge our duty and responsibility to support and facilitate the timely and unimpeded flow of health information for lawful and appropriate purposes.

Scope of Policy

This policy governs the authorization and supervision of health data-related access and activities for **CHANGES REHABILITATION LLC.**All personnel of **CHANGES REHABILITATION LLC.**must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

pdfelement

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

Assumptions

- **CHANGES REHABILITATION LLC.**hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
- **CHANGES REHABILITATION LLC.**must comply with HIPAA and the HIPAA implementing regulations pertaining to the authorization and supervision of workforce members who will be accessing individually identifiable health information as part of their work-related duties, in accordance with the requirements at § 164.308(a)(3).
- Compliance with HIPAA is mandatory and failure to comply can bring severe sanctions and penalties.
- Proper and appropriate authorization to access individually identifiable health information, and appropriate supervision of workforce members authorized to access individually identifiable health information, are essential components of a well-managed risk management system.
- Proper and appropriate authorization to access individually identifiable health information, and appropriate supervision of workforce members authorized to access individually identifiable health information, can help reduce our overall risk, and reduce the likelihood of data breaches and HIPAA violations.

Policy Statement

- It is the Policy of **CHANGES REHABILITATION LLC.**to only permit workforce members who have been appropriately authorized, to have access to individually identifiable health information.
- It is the Policy of **CHANGES REHABILITATION LLC.**to properly and appropriately supervise workforce members who have access to individually identifiable health information.
- Workforce members of **CHANGES REHABILITATION LLC.**shall have access only to the individually identifiable health information that they need in order to perform their work-related duties.
- It is the Policy of **CHANGES REHABILITATION LLC..** to fully document the authorization and supervision of all workforce members who have access to individually identifiable health information .

Procedures

Remove Watermark Now

- See Information Technology Policy IT00002.
- Annual Audit.

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **CHANGES REHABILITATION LLC**.' s Sanction Policy.

pdfelement

Remove Watermark Now

HIPAA22-Workforce Clearance Policy
Updated: 7/30/18

Introduction

CHANGES REHABILITATION LLC. has adopted this Workforce Clearance Policy in order to recognize the requirement to comply with the Health Insurance Portability and Accountability Act ("HIPAA"), as amended by the Health Information Technology for Economic and Clinical Health ("HITECH") Act of 2009 (Title XIII of division A and Title IV of division B of the American Recovery and Reinvestment Act "ARRA") and the HIPAA Omnibus Final Rule (Effective Date: March 26, 2013). We acknowledge that full compliance with the HIPAA Final Rule is required by or before September 23, 2013.

CHANGES REHABILITATION LLC. hereby acknowledges our duty and responsibility to protect the privacy and security of Individually Identifiable Health Information ("IIHI") generally, and Protected Health Information ("PHI") as defined in the HIPAA Regulations, under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under principles of general and professional ethics. We also acknowledge our duty and responsibility to support and facilitate the timely and unimpeded flow of health information for lawful and appropriate purposes.

Scope of Policy

This policy governs Workforce Clearance and Screening (pre-employment and post-employment) for **CHANGES REHABILITATION LLC.** All personnel of **CHANGES REHABILITATION LLC.**must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

pdfelement

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

Assumptions

- **CHANGES REHABILITATION LLC.** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
- **CHANGES REHABILITATION LLC..** must comply with HIPAA and the HIPAA implementing regulations pertaining to workforce clearance, in accordance with the requirements at § 164.308(a)(3).
- Providing for appropriate workforce clearance can help reduce the likelihood of data breaches and HIPAA violations.

Policy Statement

- It is the Policy of **CHANGES REHABILITATION LLC..** to provide the appropriate level of access to individually identifiable health information to all members of the workforce.
- The level of access to individually identifiable health information for workforce members shall be based upon the nature of each workforce member's job and its associated duties and responsibilities. Workforce members shall have access to all of the individually identifiable health information that they need to do their jobs, but no more access than that.
- No member of the workforce shall have access to a higher level of individually identifiable health information than the level for which they have been cleared.
- The Director of IT shall develop specific procedures to ensure that the intent of this policy is executed in fact.
- Workforce clearance shall specifically incorporate various levels of background screening to ensure that persons with criminal records do not have inappropriate access to individually identifiable health information.
- The Corporate Compliance Officer shall coordinate background screening requirements with Human Resources and legal counsel to ensure that appropriate background screening requirements are established and met, which can include pre-employment and post-employment screening.

- It is the Policy of **CHANGES REHABILITATION LLC.**to fully document all workforce clearance-related activities and efforts.

Remove Watermark Now

Procedures

- See Information Technology Policy IT00002.
- Facility is responsible for background screening.

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **CHANGES REHABILITATION LLC**.' s Sanction Policy.

pdfelement

Remove Watermark Now

HIPAA23-Access Termination Policy

Updated: 7/30/18

Introduction

CHANGES REHABILITATION LLC. has adopted this Access Termination Policy in order to recognize the requirement to comply with the Health Insurance Portability and Accountability Act ("HIPAA"), as amended by the Health Information Technology for Economic and Clinical Health ("HITECH") Act of 2009 (Title XIII of division A and Title IV of division B of the American Recovery and Reinvestment Act "ARRA") and the HIPAA Omnibus Final Rule (Effective Date: March 26, 2013). We acknowledge that full compliance with the HIPAA Final Rule is required by or before September 23, 2013.

CHANGES REHABILITATION LLC. hereby acknowledges our duty and responsibility to protect the privacy and security of Individually Identifiable Health Information ("IIHI") generally, and Protected Health Information ("PHI") as defined in the HIPAA Regulations, under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under principles of general and professional ethics. We also acknowledge our duty and responsibility to support and facilitate the timely and unimpeded flow of health information for lawful and appropriate purposes.

Scope of Policy

This policy governs the termination of individual access to individually identifiable health information and Protected Health Information for **CHANGES REHABILITATION LLC.**All personnel of **CHANGES REHABILITATION LLC.**must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

pdfelement

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

Assumptions

- **CHANGES REHABILITATION LLC.** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
- **CHANGES REHABILITATION LLC.**must comply with HIPAA and the HIPAA implementing regulations pertaining to the termination of workforce member access to individually identifiable health information and Protected Health Information, in accordance with the requirements at § 164.308(a)(3).
- Prompt and appropriate termination of workforce member access to individually identifiable health information and Protected Health Information can greatly reduce the likelihood of data breaches and HIPAA violations.

Policy Statement

- It is the Policy of **CHANGES REHABILITATION LLC.**to terminate any workforce member's access to individually identifiable health information and Protected Health Information when their employment relationship with our organization ends, or when the workforce member has been sanctioned for serious offenses or violations of policy, in accordance with our Sanction Policy.
- Termination of workforce member access to individually identifiable health information and Protected Health Information must be effected immediately upon the occurrence of a triggering event, such as termination of employment or a positive finding of a serious policy violation or HIPAA offense.
- In no case shall the termination of access to individually identifiable health information and Protected Health Information be delayed more than 30 minutes from the moment of such a triggering event.
- It is the Policy of **CHANGES REHABILITATION LLC.**to fully document all access termination-related activities, in accordance with our Documentation Policy.

Compliance and Enforcement

Remove Watermark Now

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **CHANGES REHABILITATION LLC.**'s Sanction Policy.

pdfelement

Remove Watermark Now

HIPAA24-Access Authorization Policy
Updated: 7/30/18

Introduction

CHANGES REHABILITATION LLC. has adopted this Access Authorization Policy in order to recognize the requirement to comply with the Health Insurance Portability and Accountability Act ("HIPAA"), as amended by the Health Information Technology for Economic and Clinical Health ("HITECH") Act of 2009 (Title XIII of division A and Title IV of division B of the American Recovery and Reinvestment Act "ARRA") and the HIPAA Omnibus Final Rule (Effective Date: March 26, 2013). We acknowledge that full compliance with the HIPAA Final Rule is required by or before September 23, 2013.

CHANGES REHABILITATION LLC.hereby acknowledges our duty and responsibility to protect the privacy and security of Individually Identifiable Health Information ("IIHI") generally, and Protected Health Information ("PHI") as defined in the HIPAA Regulations, under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under principles of general and professional ethics. We also acknowledge our duty and responsibility to support and facilitate the timely and unimpeded flow of health information for lawful and appropriate purposes.

Scope of Policy

This policy governs the authorization and granting of access to individually identifiable health information and Protected Health Information to workforce members of **CHANGES REHABILITATION LLC.** All personnel of **CHANGES REHABILITATION LLC..** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

pdfelement

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

Assumptions

- **CHANGES REHABILITATION LLC.** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
- **CHANGES REHABILITATION LLC.** must comply with HIPAA and the HIPAA implementing regulations pertaining to access authorization, in accordance with the requirements at § 164.308(a)(4).
- The implementation of appropriate processes to grant workforce members access to individually identifiable health information and Protected Health Information can help ensure that our uses and disclosures of individually identifiable health information are lawful and appropriate.

Policy Statement

- It is the Policy of **CHANGES REHABILITATION LLC.**to grant workforce members an appropriate level of access to individually identifiable health information that is based on their work-related duties and responsibilities.
- The level of access to individually identifiable health information and Protected Health Information granted to each member of the workforce shall be independent of the technology used to access such information, and shall apply to access through a workstation, transaction, program, process, or other mechanism.
- It is the Policy of **CHANGES REHABILITATION LLC.**to fully document all access authorization-related activities and efforts.

Procedures

- See Information Technology Policy IT00002.
- Annual Audit.

Compliance and Enforcement

Remove Watermark Now

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **CHANGES REHABILITATION LLC.**'s Sanction Policy.

pdfelement

Remove Watermark Now

HIPAA25-Access Establishment and Modification Policy
Updated: 7/30/18

Introduction

CHANGES REHABILITATION LLC.. has adopted this Access Establishment and Modification Policy in order to recognize the requirement to comply with the Health Insurance Portability and Accountability Act ("HIPAA"), as amended by the Health Information Technology for Economic and Clinical Health ("HITECH") Act of 2009 (Title XIII of division A and Title IV of division B of the American Recovery and Reinvestment Act "ARRA") and the HIPAA Omnibus Final Rule (Effective Date: March 26, 2013). We acknowledge that full compliance with the HIPAA Final Rule is required by or before September 23, 2013.

CHANGES REHABILITATION LLC. hereby acknowledges our duty and responsibility to protect the privacy and security of Individually Identifiable Health Information ("IIHI") generally, and Protected Health Information ("PHI") as defined in the HIPAA Regulations, under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under principles of general and professional ethics. We also acknowledge our duty and responsibility to support and facilitate the timely and unimpeded flow of health information for lawful and appropriate purposes.

Scope of Policy

This policy governs establishment and modification of access to individually identifiable health information and Protected Health Information for workforce members of **CHANGES REHABILITATION LLC.**All personnel of **CHANGES REHABILITATION LLC..** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

pdfelement

Assumptions

- **CHANGES REHABILITATION LLC..** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
- **CHANGES REHABILITATION LLC.** must comply with HIPAA and the HIPAA implementing regulations pertaining to the establishment and modification of workforce member access to individually identifiable health information and Protected Health Information, in accordance with the requirements at § 164.308(a)(4).
- Establishing, maintaining, and modifying appropriate levels of workforce member access to individually identifiable health information and Protected Health Information can help reduce the likelihood of data breaches and HIPAA violations.

Policy Statement

- It is the Policy of **CHANGES REHABILITATION LLC.**to provide a lawful and appropriate level of access to individually identifiable health information for each and every workforce member.
- Such access to individually identifiable health information shall be granted based on the nature and duties of the workforce member's job.
- Higher levels of access shall be provided only to those who need it.
- Any workforce member's ability to access individually identifiable health information shall be modified immediately when the nature of their job changes and requires a different level of access, whether greater or lesser.
- It is the Policy of **CHANGES REHABILITATION LLC..** to fully document all access establishment and modification- related activities and efforts, according to our Documentation Policy.

Procedures

- See Information Technology Policy IT00002, Usernames/Password Request.

Remove Watermark Now

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **ACHANGES REHABILITATION INC .**'s Sanction Policy.

pdfelement

Remove Watermark Now

HIPAA26-Security Reminders Policy
Updated: 7/30/18

Introduction

CHANGES REHABILITATION LLC. has adopted this Security Reminders Policy in order to recognize the requirement to comply with the Health Insurance Portability and Accountability Act ("HIPAA"), as amended by the Health Information Technology for Economic and Clinical Health ("HITECH") Act of 2009 (Title XIII of division A and Title IV of division B of the American Recovery and Reinvestment Act "ARRA") and the HIPAA Omnibus Final Rule (Effective Date: March 26, 2013). We acknowledge that full compliance with the HIPAA Final Rule is required by or before September 23, 2013.

CHANGES REHABILITATION LLC.hereby acknowledges our duty and responsibility to protect the privacy and security of Individually Identifiable Health Information ("IIHI") generally, and Protected Health Information ("PHI") as defined in the HIPAA Regulations, under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under principles of general and professional ethics. We also acknowledge our duty and responsibility to support and facilitate the timely and unimpeded flow of health information for lawful and appropriate purposes.

Scope of Policy

This policy governs the creation and implementation of Security Reminders for **CHANGES REHABILITATION LLC..** All personnel of **CHANGES REHABILITATION LLC..** must comply with this policy . Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

pdfelement

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

Assumptions

- **CHANGES REHABILITATION LLC.** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
- **CHANGES REHABILITATION LLC..** must comply with HIPAA and the HIPAA implementing regulations pertaining to security reminders, in accordance with the requirements at § 164.308(a)(5).
- The frequent use of appropriate security reminders and other information security awareness resources can reduce the likelihood of data breaches and HIPAA violations.

Policy Statement

- It is the Policy of **CHANGES REHABILITATION LLC..** to develop or acquire and to use appropriate information security reminders, or other information security awareness resources, on a regular basis.
- The Director of IT shall assume responsibility for developing or acquiring such reminders and resources, and for implementing a plan and program ensuring their frequent use.
- It is the Policy of **CHANGES REHABILITATION LLC.**to fully document all information security reminder-related activities and efforts, according to our Documentation Policy.

Procedures

- See Information Technology Procedure IT16.
- The Director of IT will send periodic, companywide, security reminders via the company newsletter**.**
- The Director of IT will send periodic, companywide, security reminders via email.

Compliance and Enforcement

Remove Watermark Now

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **CHANGES REHABILITATION LLC.**'s Sanction Policy.

pdfelement

Remove Watermark Now

HIPAA27-Malware Protection Policy
Updated: 7/30/18

Introduction

CHANGES REHABILITATION LLC. has adopted this Malware Protection Policy in order to recognize the requirement to comply with the Health Insurance Portability and Accountability Act ("HIPAA"), as amended by the Health Information Technology for Economic and Clinical Health ("HITECH") Act of 2009 (Title XIII of division A and Title IV of division B of the American Recovery and Reinvestment Act "ARRA") and the HIPAA Omnibus Final Rule (Effective Date: March 26, 2013). We acknowledge that full compliance with the HIPAA Final Rule is required by or before September 23, 2013.

CHANGES REHABILITATION LLC. hereby acknowledges our duty and responsibility to protect the privacy and security of Individually Identifiable Health Information ("IIHI") generally, and Protected Health Information ("PHI") as defined in the HIPAA Regulations, under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under principles of general and professional ethics. We also acknowledge our duty and responsibility to support and facilitate the timely and unimpeded flow of health information for lawful and appropriate purposes.

Scope of Policy

This policy governs Malware Protection for **CHANGES REHABILITATION LLC.**All personnel of **CHANGES REHABILITATION LLC..** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

pdfelement

Assumptions

- **CHANGES REHABILITATION LLC.** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
- **CHANGES REHABILITATION LLC.**must comply with HIPAA and the HIPAA implementing regulations pertaining to protection from so-called malware, in accordance with the requirements at § 164.308(a)(5).
- The use of appropriate techniques, technologies, and methods to protect information systems from malicious software ("malware") is a proven approach to reducing the likelihood of data breaches, system malfunctions, and HIPAA violations.

Policy Statement

- It is the Policy of **CHANGES REHABILITATION LLC.**to develop and apply a rigorous program of techniques, technologies, and methods to guard against, detect, and report the presence of malicious software.
- Responsibility for malware protection shall reside with the Director of IT who shall ensure that the most effective and appropriate techniques, technologies, and methods are continuously used to protect our information systems, and the individually identifiable health information they contain, from malicious software.
- It is the Policy of **CHANGES REHABILITATION LLC.**to fully document all malware protection-related activities and efforts, in accordance with our Documentation Policy.

Procedures

- See Information Technology Procedure IT11.

Compliance and Enforcement

Remove Watermark Now

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **CHANGES REHABILITATION LLC.**'s Sanction Policy.

pdfelement

Remove Watermark Now

HIPAA28-Log-In Monitoring Policy
Updated: 7/30/18

Introduction

CHANGES REHABILITATION LLC.. has adopted this Log-In Monitoring Policy in order to recognize the requirement to comply with the Health Insurance Portability and Accountability Act ("HIPAA"), as amended by the Health Information Technology for Economic and Clinical Health ("HITECH") Act of 2009 (Title XIII of division A and Title IV of division B of the American Recovery and Reinvestment Act "ARRA") and the HIPAA Omnibus Final Rule (Effective Date: March 26, 2013). We acknowledge that full compliance with the HIPAA Final Rule is required by or before September 23, 2013.

CHANGES REHABILITATION LLC. hereby acknowledges our duty and responsibility to protect the privacy and security of Individually Identifiable Health Information ("IIHI") generally, and Protected Health Information ("PHI") as defined in the HIPAA Regulations, under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under principles of general and professional ethics. We also acknowledge our duty and responsibility to support and facilitate the timely and unimpeded flow of health information for lawful and appropriate purposes.

Scope of Policy

This policy governs Log-In Monitoring for **CHANGES REHABILITATION LLC..** All personnel of **CHANGES REHABILITATION LLC..** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

pdfelement

Assumptions

- **CHANGES REHABILITATION LLC.** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
- **CHANGES REHABILITATION LLC.** must comply with HIPAA and the HIPAA implementing regulations pertaining to log-in monitoring, in accordance with the requirements at § 164.308(a)(5).
- Regular monitoring of log-ins and log-in attempts is a proven approach to controlling access to sensitive information systems and data, and to detecting inappropriate information systems activity.

Policy Statement

- It is the Policy of **CHANGES REHABILITATION LLC.**to establish a program of regular monitoring and review of log- ins and log-in attempts.
- The Director of IT shall assume responsibility for log-in monitoring and analysis, and for ensuring that such activities are executed on a continuous basis.
- Discrepancies and potentially inappropriate or illegal activities shall immediately be brought to the attention of senior management, legal counsel, and/or Human Resources, as appropriate.
- It is the Policy of **CHANGES REHABILITATION LLC.**to fully document all log-in monitoring-related activities and efforts, in accordance with our Documentation Policy.

Procedures

- See Information Technology Procedures IT06 and IT07.

Compliance and Enforcement

Remove Watermark Now

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **CHANGES REHABILITATION LLC.**'s Sanction Policy.

pdfelement

Remove Watermark Now

HIPAA29-Password Management Policy
Updated: 7/30/18

Introduction

CHANGES REHABILITATION LLC. has adopted this Password Management Policy in order to recognize the requirement to comply with the Health Insurance Portability and Accountability Act ("HIPAA"), as amended by the Health Information Technology for Economic and Clinical Health ("HITECH") Act of 2009 (Title XIII of division A and Title IV of division B of the American Recovery and Reinvestment Act "ARRA") and the HIPAA Omnibus Final Rule (Effective Date: March 26, 2013). We acknowledge that full compliance with the HIPAA Final Rule is required by or before September 23, 2013.

ATRIUM CENTERS LLC. hereby acknowledges our duty and responsibility to protect the privacy and security of Individually Identifiable Health Information ("IIHI") generally, and Protected Health Information ("PHI") as defined in the HIPAA Regulations, under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under principles of general and professional ethics. We also acknowledge our duty and responsibility to support and facilitate the timely and unimpeded flow of health information for lawful and appropriate purposes.

Scope of Policy

This policy governs information systems Password Management for **CHANGES REHABILITATION LLC.**All personnel of **CHANGES REHABILITATION LLC.**must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

pdfelement

Assumptions

- **CHANGES REHABILITATION LLC.** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
- **CHANGES REHABILITATION LLC.** must comply with HIPAA and the HIPAA implementing regulations pertaining to password management, in accordance with the requirements at § 164.308(a)(5).
- The creation and management of strong passwords is one of the simplest and most effective methods of protecting access to electronic systems containing, transmitting, receiving, or using individually identifiable health information.
- The monitoring of successful and unsuccessful Log-In attempts is a well established method of detecting malicious intrusions, and intrusion attempts, into information systems by unauthorized persons.

Policy Statement

- It is the Policy of **CHANGES REHABILITATION INC** to require the use of strong passwords and pass-phrases by all workforce members who access, use, or maintain systems that contain, transmit, receive , or use individually identifiable health information.
- The responsibility for implementing this policy and any attendant procedures is hereby assigned to the Director of IT, who shall develop and implement this policy.

Procedures

- All passwords or pass-phrases used to access systems containing, transmitting, receiving, or using individually identifiable health information shall be a minimum of six (8) characters in length, and must include non-alphanumeric characters and symbols in them.
- Passwords and pass-phrases must or should be changed by users at least every 90 days.

- In the event of an information system compromise, as determined by the Director of IT, some or all workforce-member passwords and pass-phrases may need to be changed. This determination shall be made by the Director of IT.
- Under no circumstances shall passwords or pass-phrases be written down and kept at or near computers and workstations where they may be found by others. Passwords and pass-phrases may, however, be written down and stored in a workforce member's wallet or purse, if the password or pass-phrase is thus afforded protection equal to the protection afforded to workforce members' cash, credit cards, and other critical documents.
- Any workforce member who loses, misplaces, forgets or experiences any compromise of their password or pass-phrase shall immediately notify the Help Desk, or, if they are unavailable, shall notify the Director of IT. Such notification of password or pass-phrase compromise must be made *immediately* to the contact(s) indicated herein, but in no case shall such notification be delayed more than one hour.
- Proper password management shall be emphasized in HIPAA training programs, in security reminders, and in any HIPAA awareness resources used by this organization.
- See Information Technology Policy IT00012.
- Corporate Compliance Audit.

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **CHANGES REHABILITATION INC**'s Sanction Policy.

Remove Watermark Now
pdfelement

Remove Watermark Now

HIPAA30-Policy on Security Incident Procedures

Updated: 7/30/18

Introduction

CHANGES REHABILITATION LLC. has adopted this Policy regarding Security Incident Procedures in order to recognize the requirement to comply with the Health Insurance Portability and Accountability Act ("HIPAA"), as amended by the Health Information Technology for Economic and Clinical Health ("HITECH") Act of 2009 (Title XIII of division A and Title IV of division B of the American Recovery and Reinvestment Act "ARRA") and the HIPAA Omnibus Final Rule (Effective Date: March 26, 2013). We acknowledge that full compliance with the HIPAA Final Rule is required by or before September 23, 2013.

CHANGES REHABILITATION INC hereby acknowledges our duty and responsibility to protect the privacy and security of Individually Identifiable Health Information ("IIHI") generally, and Protected Health Information ("PHI") as defined in the HIPAA Regulations, under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under principles of general and professional ethics. We also acknowledge our duty and responsibility to support and facilitate the timely and unimpeded flow of health information for lawful and appropriate purposes.

Scope of Policy

This policy governs responses to Security Incidents involving the breach or compromise of Protected Health Information for **CHANGES REHABILITATION INC** All personnel of **CHANGES REHABILITATION LLC.** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

pdfelement

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

Assumptions

- **CHANGES REHABILITATION INC** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
- **CHANGES REHABILITATION INC** must comply with HIPAA and the HIPAA implementing regulations pertaining to security incident procedures, in accordance with the requirements at § 164.308(a)(6) and at § 164.400 to 164.414.
- Appropriate responses to security incidents may include, but are not limited to:
  - Rapid identification and classification of the severity of security incidents.
  - Determination of the actual risk to individually identifiable health information, and the subject(s) thereof.
  - Repairing, patching, or otherwise correcting the condition or error that created the security incident.
  - Retrieving or limiting the dissemination of individually identifiable health information, if possible.
  - Determining if the security incident rises to the level of a reportable breach under the HIPAA regulations.
  - Making a lawful and appropriate report of a breach, if required, to the appropriate parties. Appropriate parties to whom breaches must be reported, as defined by HIPAA regulations, may include, but are not limited to:
    - Patients
    - Consumers
    - Regulatory Authorities, including HHS and/or the Federal Trade Commission
    - Law Enforcement
    - The local media, if necessary and required by law
  - Mitigating any harmful effects of the security incident.
  - Fully documenting security incidents, along with their causes and our responses.

Remove Watermark Now

- Expanding our knowledge of security incident prevention, through research, analyses of secu incidents, and improved training and awareness programs for workforce members.

- Compliance with HIPAA's data protection requirements is mandatory and failure to comply can bring severe sanctions and penalties.

Policy Statement

- It is the Policy of **CHANGES REHABILITATION INC** to rapidly identify and appropriately respond to all security incidents, regardless of their severity.
- Responsibility for responding to and managing security incidents shall reside with Corporate Compliance Officer and the Director of IT.
- The Corporate Compliance Officer and the Director of IT shall develop specific forms and procedures that shall be implemented in response to security incidents.
- It is the Policy of **CHANGES REHABILITATION LLC.**to fully document all security incidents and our responses thereto, in accordance with our Documentation Policy and HIPAA requirements.

Procedures

- See Information Technology Policies IT00009, IT00012 and IT00014.

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **CHANGES REHABILITATION LLC.**' s Sanction Policy.

pdfelement

Remove Watermark Now

HIPAA31-Data Backup Policy
Updated: 7/30/18

Introduction

CHANGES REHABILITATION LLC. has adopted this Data Backup Policy in order to recognize the requirement to comply with the Health Insurance Portability and Accountability Act ("HIPAA"), as amended by the Health Information Technology for Economic and Clinical Health ("HITECH") Act of 2009 (Title XIII of division A and Title IV of division B of the American Recovery and Reinvestment Act "ARRA") and the HIPAA Omnibus Final Rule
(Effective Date: March 26, 2013). We acknowledge that full compliance with the HIPAA Final Rule is required by or before September 23, 2013.

CHANGES REHABILITATION INC hereby acknowledges our duty and responsibility to protect the privacy and security of Individually Identifiable Health Information ("IIHI") generally, and Protected Health Information ("PHI") as defined in the HIPAA Regulations, under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under principles of general and professional ethics. We also acknowledge our duty and responsibility to support and facilitate the timely and unimpeded flow of health information for lawful and appropriate purposes.

Scope of Policy

This policy governs Data Backups for **CHANGES REHABILITATION INC** All personnel of **CHANGES REHABILITATION LLC.** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

Assumptions

- **CHANGES REHABILITATION INC** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
  - **CHANGES REHABILITATION INC** must comply with HIPAA and the HIPAA implementing regulations pertaining to data backups, in accordance with the requirements at § 164.308(a)(7) and elsewhere in the Regulations.
- The ability to create and maintain retrievable, exact copies of individually identifiable health information generally, and Electronic Protected Health Information specifically, is a critical element of our business operations and our ability to respond to unexpected negative events.
- The storage of data backups in a separate location, removed from our normal business operations ("offsite") is an essential element of any successful data backup plan.
- Timely access to health information is crucial to providing high quality health care, and to our business operations.
- Physicians, healthcare providers and others must have immediate, around-the-clock access to patient information.
- No existing media are absolutely guaranteed to provide long-term storage without loss or corruption of data.
- A number of risks to health information exist, such as power spikes or outages, fire, flood, or other natural disaster, viruses, hackers, and improper acts by employees and others.

Policy Statement

- It is the Policy of **CHANGES REHABILITATION LLC.** to create and maintain complete, retrievable, exact backups of all individually identifiable health information generally, and Electronic Protected Health Information specifically, held, processed, or stored in the course of business operations, in full compliance with all the requirements of HIPAA.
- All data backups shall be created and maintained in such manner as to ensure the maximum degree of data integrity, availability, and confidentiality are maintained at all times.

pdfelement

Remove Watermark Now

Procedures

- The **Director of IT** is responsible for performing daily backups on **CHANGES REHABILITATION INC**'s network, including shared drives containing application data, patient information, financial data, and crucial system information.
- **CHANGES REHABILITATION LLC.** will back up all such data automatically, per **Unitrend's** programmed standards, nightly.
- The **Director of IT,** the system administrator, or their designees will use **Unitrend's** reporting utilities at the start of each business day to validate the accuracy, completeness, and integrity of the backup performed the previous night.
- Individuals so validating the backup will generate daily reports and log them in the network log in the system administrator's office. The system administrator will maintain such reports for a minimum of 30 days.
- Any errors will be acted upon immediately. Responsible personnel will use contract technical support as needed to resolve problems and ensure the validity of backup data.
- Responsible personnel will clean backup unit(s) according to the manufacturer's recommended guidelines, currently once per week.
- The **Director of IT** will ensure replacement of media according to manufacturer's recommended guidelines, currently annually.
- The **Director of IT** is responsible for testing the validity of backup data and the ability to restore data in the event of a computer system problem, failure, or other disaster at least quarterly and more often if necessary to ensure data integrity, availability, and confidentiality.
- Successful restore functions must be logged in the network log. Any problems identified during the restore function must be acted on immediately and no later than the same business day that they occur. Responsible personnel will use contract technical support as needed to resolve problems and ensure the validity of backup data.
- All personnel who detect or suspect a data backup problem should immediately report the same to the **Director of IT**. Such personnel should follow up immediate notification with a written memorandum that includes the following information:
    - Narrative of the data backup problem.
    - How long the problem has existed.
    - Suggested solutions.
- See Information Technology Procedure IT08.
- Annual Audit.

pdfelement

Compliance and Enforcement

All information technology managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **CHANGES REHABILITATION LLC.**'s Sanction Policy.

Remove Watermark Now

HIPAA32-Disaster Recovery Policy
Updated: 7/30/18

Introduction

CHANGES REHABILITATION INC has adopted this Disaster Recovery Policy in order to recognize the requirement to comply with the Health Insurance Portability and Accountability Act ("HIPAA"), as amended by the Health Information Technology for Economic and Clinical Health ("HITECH") Act of 2009 (Title XIII of division A and Title IV of division B of the American Recovery and Reinvestment Act "ARRA") and the HIPAA Omnibus Final Rule (Effective Date: March 26, 2013). We acknowledge that full compliance with the HIPAA Final Rule is required by or before September 23, 2013.

CHANGES REHABILITATION INChereby acknowledges our duty and responsibility to protect the privacy and security of Individually Identifiable Health Information ("IIHI") generally, and Protected Health Information ("PHI") as defined in the HIPAA Regulations, under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under principles of general and professional ethics. We also acknowledge our duty and responsibility to support and facilitate the timely and unimpeded flow of health information for lawful and appropriate purposes.

Scope of Policy

This policy governs contingency Disaster Recovery Planning for **CHANGES REHABILITATION LLC.**All personnel of **CHANGES REHABILITATION INC** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

pdfelement

Assumptions

- **CHANGES REHABILITATION LLC.** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
- **CHANGES REHABILITATION INC** must comply with HIPAA and the HIPAA implementing regulations pertaining to disaster recovery, in accordance with the requirements at § 164.308(a)(7).
- HIPAA requires **CHANGES REHABILITATION INC** to establish and implement processes and procedures for responding effectively to emergencies or other occurrences (fire, vandalism, system failure, and natural disaster, etc.) that damage systems containing electronic protected health information.
- A disaster may occur at any time, not necessarily during work hours.
- **CHANGES REHABILITATION INC** must remain operational with as little disruption of business operations and patient care as possible.
- Continuity of patient care requires uninterrupted access to patient information.
- In a dangerous emergency, evacuating personnel has priority over preserving information assets.
- The following conditions can destroy or disrupt **CHANGES REHABILITATION INC**'s information systems:
  - Power interruption.
  - Fire.
  - Water.
  - Weather and other natural phenomena, such as earthquakes.
  - Sabotage and vandalism.
  - Terrorism.

Policy Statement

It is the policy of **CHANGES REHABILITATION INC** to establish and implement processes and procedures to create and maintain retrievable exact copies of electronic protected health information.

Procedures

Remove Watermark Now

Preventive Measures

- The **Director of IT** and or their designee(s) shall ensure that the following preventive measures, as applicable, are implemented and documented:
  - Back up computerized files according to our Data Backup Policy.
  - Test integrity of backup system no less than quarterly, according to our Data Backup Policy.
  - Store media properly. For example, laser discs must be stored in sleeves of plastic, paper, or combination of the two, placed in cardboard jackets or boxes, and stored on edge on metal shelving, properly labeled.
  - Color-code all media as to priority of evacuation: red is first priority; yellow is second priority; green is third priority.
  - In the event of a fire or flood, turn off and unplug electrical equipment when contact with water is imminent.
  - In the event of a fire or flood, seal room(s) to contain fire or water and/or use strategies to protect information and equipment from fire or from water falling from above as appropriate.
  - Training in disaster preparation and recovery, and knowledge of responsibilities in the event of a disaster.

- The **Director of IT** must implement and document the following:
  - Ensure that major hardware is covered under **CHANGES REHABILITATION LLC.**'s property and casualty, and or other appropriate insurance policy or policies.
  - Ensure that uninterruptible power supply, fire protection, and other disaster prevention systems are functioning properly, periodically check these systems, and train employees in their use.

Priority Tasks during Emergencies

As applicable, and under appropriate circumstances, all workforce members should:

- Remain calm.
- Activate the alarm. That is, pull the fire alarm or call 911 as appropriate.
- Evacuate if necessary. If personnel are injured, ensure their evacuation and call emergency assistance as necessary.
- If a fire occurs that you believe you can fight, use the nearest fire extinguisher.
- If safe, close all doors as you leave.
- Obtain portable phone(s) to communicate.
- Notify concerned fire, police, security, administration, and others as necessary.
- Notify other departments of situation and emergency protocols.
- If computers have not automatically powered down, initiate procedures to orderly shut down systems, when possible.
- If a fire or flood occurs, disconnect power if possible.
- If a fire or flood occurs, try to prevent further damage from water by covering areas with plastic sheets with adequate drainage.
- Move records/equipment/storage media away from area being flooded. Organize health information logically and label clearly for continued access.
- Arrange for transportation of paper records to a salvage, restoration, or reconstruction company.
- Respond to requests for records via portable phone rather than computer.
- Continue to provide patient charts as requested by physicians or other parties.

Priority Disaster Recovery Tasks

As applicable, and under appropriate circumstances, all workforce members should:

- Prevent personnel from entering the area until officials or building inspectors have determined that the area is safe to reenter.
- Not permit unauthorized personnel to enter the affected area.
- Determine the extent of the damage and whether additional equipment/supplies are needed.
- Determine how long it will be before service can be restored, and notify departments.
- Replace hardware as necessary to restore service.
- Work with vendors as necessary to ensure that support is given to restore service.
- Notify insurance carriers.
- Retrieve and upload backup files if necessary to restore service.
- Air-dry floppy disks, if any, using a hair dryer on "air," not "heat." When dry, copy disk.

pdfelement

- For water damage, wipe off CD-ROMs and laser discs with distilled water, working out from the center in a straight line, and then wipe off water or dirt with a soft, dry, lint-free cloth. Air-dry. Do not use a hairdryer. For dirt or smoke damage, wipe out from the center with a clean, soft cloth. Then wash off any remaining dirt with distilled water.
- Remove water-damaged paper records by the wettest first. Freeze wet items to stabilize.
- Wrap paper records to prevent them from sticking together. Label the wrapped records.
- Contact fire, water, and storm damage Restoration Company. Contract for services as needed.
- Reconstruct/reacquire documents from the following:
  - Dictation system.
  - Word processing system.
  - Computer system.
  - Holders of document copies.
- Move records and equipment back to home location.
- Catch up on filing.
- Ensure that backup procedures are followed.
- Document data that cannot be recovered in patient record.
- Meet with management and staff to identify opportunities for improvement.

Additional Disaster Recovery Tasks

The following tasks must be assigned to specific persons or positions:

- ❑ Determine whether additional equipment and supplies are needed.
- ❑ Notify vendors or service representatives if there is need for immediate delivery of components to bring the computer systems to an operational level even in a degraded mode.
- ❑ If necessary, check with other vendors to see whether they can provide faster delivery.
- ❑ Rush order any supplies and equipment necessary.
- ❑ Notify personnel that an alternate site will be necessary and where it is located.
- ❑ Coordinate moving equipment and support personnel to the alternate site.
- ❑ Bring recovery materials from offsite storage to the alternate site.
- ❑ As soon as hardware is up to specifications to run the operating system, load software and run necessary tests.
- ❑ Determine priorities of software that must be available and load those packages in order. Post these priorities in a conspicuous location.
- ❑ Prepare backup materials and return them to the offsite storage area.
- ❑ Set up operations at the alternate site if necessary.
- ❑ Coordinate activities to ensure that the most critical tasks, such as immediate patient care, are being supported as needed.
- ❑ Ensure that periodic backup procedures are followed according to our Data Backup Policy.
- ❑ Plan to phase in all critical support.
- ❑ Keep administration, medical staff, information personnel, and others informed of the status of the emergency mode operations.
- ❑ Coordinate with administration and others for continuing support and ultimate restoration of normal operations.
- ❑ See Information Technology Procedure IT08.
- ❑ Annual Audit.

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **CHANGES REHABILITATION LLC**.'s Sanction Policy.

Remove Watermark Now
pdfelement

Remove Watermark Now

HIPAA33-Emergency Mode Operations Policy
Updated: 7/30/18

Introduction

CHANGES REHABILITATION INC has adopted this Emergency Mode Operations Policy in order to recognize the requirement to comply with the Health Insurance Portability and Accountability Act ("HIPAA"), as amended by the Health Information Technology for Economic and Clinical Health ("HITECH") Act of 2009 (Title XIII of division A and Title IV of division B of the American Recovery and Reinvestment Act "ARRA") and the HIPAA Omnibus Final Rule (Effective Date: March 26, 2013). We acknowledge that full compliance with the HIPAA Final Rule is required by or before September 23, 2013.

CHANGES REHABILITATION INC hereby acknowledges our duty and responsibility to protect the privacy and security of Individually Identifiable Health Information ("IIHI") generally, and Protected Health Information ("PHI") as defined in the HIPAA Regulations, under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under principles of general and professional ethics. We also acknowledge our duty and responsibility to support and facilitate the timely and unimpeded flow of health information for lawful and appropriate purposes.

Scope of Policy

This policy governs Emergency Mode Operations and planning for **CHANGES REHABILITATION INC** All personnel of **CHANGES REHABILITATION INC** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

pdfelement

Assumptions

- **CHANGES REHABILITATION INC** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
- **CHANGES REHABILITATION INC** must comply with HIPAA and the HIPAA implementing regulations pertaining to emergency mode operations planning, in accordance with the requirements at § 164.308(a)(7).
- Individually identifiable health information must be protected during emergencies, even as it is protected during normal operations. This Emergency Mode Operations Policy is designed to ensure the protection and availability of individually identifiable health information and Protected Health Information during emergencies requiring **CHANGES REHABILITATION INC**to operate in "emergency mode".
- Our Emergency Mode Operations Plan must be implemented and executed in coordination with other emergency and/or disaster plans and procedures, as appropriate and necessary.

Policy Statement

- It is the Policy of **CHANGES REHABILITATION INC** to establish this Emergency Mode Operations Policy to implement procedures to enable continuation of critical business processes for the protection of individually identifiable health information while operating in emergency mode .
- It is the Policy of **CHANGES REHABILITATION LLC.**to fully document all emergency planning and preparedness activities and efforts, in accordance with our Documentation Policy.
- Our Emergency Mode Operations Plan shall be executed whenever **CHANGES REHABILITATION LLC.**must operate in "emergency mode".
- "Emergency Mode" shall be in effect and activated whenever one or more of the following conditions applies:
    - Electrical power is unavailable for more than eight hours.
    - Fire, flood, storm or other natural disaster renders our normal business facility unavailable or unusable for more than eight hours.

- Any other condition renders our normal business facility unavailable or unusable for more than eight hours.

Remove Watermark Now

Procedures

Responsibility and Role Assignments

The following personnel are hereby assigned to lead the functions listed below during emergency mode operations...

Function	Individual(s) Assigned
Telephones Outbound	Director of IT
Telephones Inbound	Director of IT
Computing Resources	Director of IT
U.S. Mail	Facility Program Director/Assistant
Couriers (FedEx, etc.)	Facility Program Director/Assistant
Internet and Email	Director of IT
Customer/Patient Contact	Facility Program Director/Assistant
Medical Records	Facility Program Director/Assistant
Other Business Records	Program Director/Assistant
Legal Issues	Governing Board/Director of Risk Management
Transportation	Facility Program Director
Internal Communications	Chief Operating Officer
Physical Security	Director of Maintenance
Utilities Restoration	Facility Program Director
Remediation & Restoration	Chief Operating Officer
Vendor/Partner Relations	Facility Program Director
Media Relations	Marketing Director

pdfelement

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **CHANGES REHABILITATION INC**s Sanction Policy.

Remove Watermark Now

HIPAA34-Testing and Revision of Contingency and Emergency Plans and Procedures

Updated: 7/30/18

Introduction

CHANGES REHABILITATION INC has adopted this Policy on Testing and Revision of Contingency and Emergency Plans and Procedures in order to recognize the requirement to comply with the Health Insurance Portability and Accountability Act ("HIPAA"), as amended by the Health Information Technology for Economic and Clinical Health ("HITECH") Act of 2009 (Title XIII of division A and Title IV of division B of the American Recovery and Reinvestment Act "ARRA") and the HIPAA Omnibus Final Rule (Effective Date: March 26, 2013). We acknowledge that full compliance with the HIPAA Final Rule is required by or before September 23, 2013.

CHANGES REHABILITATION INChereby acknowledges our duty and responsibility to protect the privacy and security of Individually Identifiable Health Information ("IIHI") generally, and Protected Health Information ("PHI") as defined in the HIPAA Regulations, under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under principles of general and professional ethics. We also acknowledge our duty and responsibility to support and facilitate the timely and unimpeded flow of health information for lawful and appropriate purposes.

Scope of Policy

This policy governs Testing and Revision of Contingency and Emergency Plans and Procedures for **CHANGES REHABILITATION INC** All personnel of **CHANGES REHABILITATION INC** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

pdfelement

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

Assumptions

- ❑ **CHANGES REHABILITATION INC** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
- ❑ **CHANGES REHABILITATION INC** must comply with HIPAA and the HIPAA implementing regulations pertaining to the testing and revision of emergency and contingency plans and procedures, in accordance with the requirements at § 164.308(a)(7).
- ❑ Emergency and contingency plans, and the procedures associated with them, must be periodically tested and revised to ensure that they meet the emergency preparedness needs of **CHANGES REHABILITATION LLC.**
- ❑ Individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA) must be afforded the same degree of security and privacy protection during the execution of any emergency or contingency plan as such information would receive during normal business operations.

Policy Statement

- ❑ It is the Policy of **CHANGES REHABILITATION LLC.** to periodically test, and revise as necessary, all emergency preparedness plans, including emergency and contingency plans.
- ❑ It is the Policy of **CHANGES REHABILITATION LLC.** that all individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA) shall be afforded the same degree of security and privacy protection during the execution of any emergency or contingency plan as such information would receive during normal business operations.

Procedures

- ❑ Emergency and contingency plans are the responsibility of the Director of IT, who shall ensure that all such plans are up-to-date and meet our emergency preparedness requirements.

- Emergency and contingency plans shall be reviewed, and revised if necessary, at least annually. Cop of all such plans shall remain on file and be available to all personnel.
- Emergency and contingency plans shall be rehearsed, with all team members participating in such rehearsals, at least annually.
- The Director of IT shall fully document all emergency preparedness plans, including emergency and contingency plans and all the revisions thereto, in accordance with our Documentation Policy and the requirements of HIPAA.

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **CHANGES REHABILITATION LLC.** s Sanction Policy.

Remove Watermark Now
pdfelement

Remove Watermark Now

HIPAA35-Policy on Data and Applications Criticality Analysis

Updated: 7/30/18

Introduction

CHANGES REHABILITATION LLC. has adopted this Policy on Data and Applications Criticality Analyses in order to recognize the requirement to comply with the Health Insurance Portability and Accountability Act (" HIPAA"), as amended by the Health Information Technology for Economic and Clinical Health ("HITECH") Act of 2009 (Title XIII of division A and Title IV of division B of the American Recovery and Reinvestment Act " ARRA") and the HIPAA Omnibus Final Rule (Effective Date: March 26, 2013). We acknowledge that full compliance with the HIPAA Final Rule is required by or before September 23, 2013.

ACHANGES REHABILITATION LLC hereby acknowledges our duty and responsibility to protect the privacy and security of Individually Identifiable Health Information ("IIHI") generally, and Protected Health Information (" PHI") as defined in the HIPAA Regulations, under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under principles of general and professional ethics . We also acknowledge our duty and responsibility to support and facilitate the timely and unimpeded flow of health information for lawful and appropriate purposes.

Scope of Policy

This policy governs Data and Applications Criticality Analyses for **CHANGES REHABILITATION LLC.** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

pdfelement

Assumptions

- **CHANGES REHABILITATION LLC.** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
- **CHANGES REHABILITATION LLC.** must comply with HIPAA and the HIPAA implementing regulations pertaining to the analysis of the relative criticality of both data and applications , in accordance with the requirements at § 164.308(a)(7).
- A thorough assessment and understanding of the relative criticality of both data and applications is essential to emergency preparedness, and to effectively protecting individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA) during emergencies and during normal business operations.

Policy Statement

- It is the Policy of **CHANGES REHABILITATION LLC.** to assess the relative criticality of all data, so that such data may be properly protected during emergencies and during normal business operations.

Procedures

- Data to be subject to criticality analysis shall include individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).
- Criticality analysis shall be the responsibility of the Director of IT, who shall work in cooperation with legal counsel and other internal parties as necessary to execute and document such analyses.
- Criticality analyses shall determine and document the relative criticality of each type or category of data and applications that **CHANGES REHABILITATION LLC.**possesses and/or uses to the continuity and success of our operations.

- The most critical data and applications shall be given the given the highest priority in terms of investm and emergency protection preparations; with less critical categories or types of data and applications receiving proportionately less funding and attention, as appropriate.
- In conducting data and applications analyses, the Director of IT shall employ the technical guidance and recommendations of the National Institute of Standards and Technology ("NIST"), and/or other information technology "best practices", as appropriate.
- The Director of IT shall fully document all analyses of the relative criticality of both data and applications, in accordance with our Documentation Policy and the requirements of HIPAA.

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **CHANGES REHABILITATION LLC.**' s Sanction Policy.

Remove Watermark Now
pdfelement

Remove Watermark Now

HIPAA36-Policy on Evaluating the Effectiveness of Security Policies and Procedures

Updated: 7/30/18

Introduction

CHANGES REHABILITATION LLC. has adopted this Policy on Determining the Effectiveness of Security Policies and Procedures in order to recognize the requirement to comply with the Health Insurance Portability and Accountability Act ("HIPAA"), as amended by the Health Information Technology for Economic and Clinical Health ("HITECH") Act of 2009 (Title XIII of division A and Title IV of division B of the American Recovery and Reinvestment Act "ARRA") and the HIPAA Omnibus Final Rule (Effective Date: March 26, 2013). We acknowledge that full compliance with the HIPAA Final Rule is required by or before September 23, 2013.

CHANGES REHABILITATION LLC.hereby acknowledges our duty and responsibility to protect the privacy and security of Individually Identifiable Health Information ("IIHI") generally, and Protected Health Information ("PHI") as defined in the HIPAA Regulations, under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under principles of general and professional ethics. We also acknowledge our duty and responsibility to support and facilitate the timely and unimpeded flow of health information for lawful and appropriate purposes.

Scope of Policy

This policy governs periodic Evaluations of the Effectiveness of Security Policies and Procedures for **CHANGES REHABILITATION LLC.** All personnel of **CHANGES REHABILITATION LLC.**must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

pdfelement

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

Assumptions

- **CHANGES REHABILITATION LLC.** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
- **CHANGES REHABILITATION LLC.**must comply with HIPAA and the HIPAA implementing regulations pertaining to the periodic evaluation of the effectiveness of security policies and procedures, in accordance with the requirements at § 164.308(a)(8).
- Security policies and procedures, including emergency and contingency plans and procedures, must be evaluated periodically to determine their potential effectiveness in genuine emergencies.

Policy Statement

- It is the Policy of **CHANGES REHABILITATION LLC.** to periodically evaluate security policies and procedures, including emergencand contingency plans and procedures, in order to improve their effectiveness.

Procedures

- It shall be the responsibility of the Corporate Compliance Officer and the Director of IT to periodically conduct such technical and nontechnical evaluations.
- The Corporate Compliance Officer and the Director of IT shall work in coordination with legal counsel, information technology, senior management, and any other persons, departments or parties necessary in order to conduct such evaluations.
- Such technical and nontechnical evaluations shall be conducted at least every six months.
- The results of such technical and nontechnical evaluations shall be internally published and shall be available to senior management and to all parties with responsibility for emergency preparedness.
- The purpose of such evaluations is to improve the effectiveness of our security policies and procedures, including emergency and contingency plans and procedures, so that they best protect our business, our

assets, our personnel, and the individually identifiable health information, including Protected Health Information (“PHI”, as defined by HIPAA) that we possess or use.

- ❑ The Corporate Compliance Officer or the Director of IT shall fully document our periodic technical and nontechnical evaluations to determine the effectiveness of our security policies and procedures, including emergency and contingency plans and procedures, in accordance with our Documentation Policy and the requirements of HIPAA.
- ❑ Annual Audit.

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **CHANGES REHABILITATION LLC.**’s Sanction Policy.

Remove Watermark Now
pdfelement

Remove Watermark Now

HIPAA37-Business Associates Policy
Updated: 7/30/18

Introduction

CHANGES REHABILITATION LLC. has adopted this Business Associates Policy in order to recognize the requirement to comply with the Health Insurance Portability and Accountability Act ("HIPAA"), as amended by the Health Information Technology for Economic and Clinical Health ("HITECH") Act of 2009 (Title XIII of division A and Title IV of division B of the American Recovery and Reinvestment Act "ARRA") and the HIPAA Omnibus Final Rule (Effective Date: March 26, 2013). We acknowledge that full compliance with the HIPAA Final Rule is required by or before September 23, 2013.

CHANGES REHABILITATION LLC.hereby acknowledges our duty and responsibility to protect the privacy and security of Individually Identifiable Health Information ("IIHI") generally, and Protected Health Information ("PHI") as defined in the HIPAA Regulations, under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under principles of general and professional ethics. We also acknowledge our duty and responsibility to support and facilitate the timely and unimpeded flow of health information for lawful and appropriate purposes.

Scope of Policy

This policy governs relationships with, and operations involving Business Associates for **CHANGES REHABILITATION LLC.** All personnel of **CHANGES REHABILITATION LLC.** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

pdfelement

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

Assumptions

- **ATRIUM CENTERS LLC.** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
- **CHANGES REHABILITATION LLC.** must comply with HIPAA and the HIPAA implementing regulations pertaining to Business Associates, in accordance with the requirements at § 164.308(b)(1), § 164.410, § 164.502(e), § 164.504(e), and HITECH Act § 13401.
- In cooperation with our organization, Business Associates work with, use, transmit, and/or receive individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA), which is afforded specific protections under HIPAA.
- **CHANGES REHABILITATION LLC.** has the primary responsibility in all Business Associate relationships to ensure that individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA), is properly protected and safeguarded.
- The HIPAA ("Omnibus") Final Rule specifically identifies the following types of entities as business associates:
  - Subcontractors.
  - Patient safety organizations.
  - HIOs -- Health Information Organizations (and similar organizations). HHS declined to specifically define HIOs in the Omnibus Rule, but chose the term "HIO" because it includes both Health Information Exchanges (HIEs) and regional health information organizations.
  - E-Prescribing gateways.
  - PHRs -- Personal Health Record vendors that provide services on behalf of a covered entity. PHR vendors that do not offer PHRs on behalf of CEs are not BAs.
  - Other firms or persons who "facilitate data transmission" that requires routine access to PHI.
- The "Minimum Necessary Standard" now applies directly to Business Associates. HIPAA now applies the Minimum Necessary standard directly to Business Associates and their subcontractors. When using, disclosing or requesting PHI, all these entities must make reasonable efforts to limit Protected Health

Information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

- Subcontractors of Business Associates are now Business Associates themselves. A subcontractor is defined as a person or entity to whom a Business Associate delegates a function, activity, or service involving Protected Health Information, and who is not a member of the Business Associate's own workforce.
- **CHANGES REHABILITATION LLC.** is not required to enter into a contract or other arrangement with a Business Associate that is a subcontractor. That is the responsibility of the primary or first-tier Business Associate.

Policy Statement

- It is the Policy of **CHANGES REHABILITATION LLC..** to establish and maintain business and working relationships with Business Associates that are in full compliance with all the requirements of HIPAA Final "Omnibus" Rule.

Procedures

- Responsibility for maintaining appropriate and lawful relationships with Business Associates shall reside with the Corporate Compliance Officer, who shall ensure that all aspects of our Business Associate relationships are appropriate and lawful, and who shall ensure that individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA), is properly protected and safeguarded by our Business Associates.
- With regard to Business Associates, the duties and responsibilities of the Corporate Compliance Officer shall include, but are not limited to the following:
  - Ensure that all Business Associate contracts meet all HIPAA requirements and standards, including those requirements and standards amended by the HITECH Act, the HIPAA "Omnibus" Final Rule, and any requirements of State laws in the state(s) where we operate.
  - Ensure that individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA), is properly protected and safeguarded by our Business Associates.
  - Ensure that Business Associates understand the importance and necessity of protecting individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA), whether in electronic form ("ePHI") or hardcopy form.
  - Ensure that Business Associates have proper and appropriate safeguards in place for individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA), before entrusting such information to them.
  - Ensure that Business Associates understand and are properly prepared to detect and respond to breaches of individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).
- The Corporate Compliance Officer shall fully document all Business Associate-related contracts and activities, in accordance with our Documentation Policy and the requirements of HIPAA.

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **CHANGES REHABILITATION LLC.**' s Sanction Policy.

Remove Watermark Now
Pathfinder

Remove Watermark Now

HIPAA38-Contingency Operations Policy
Updated: 7/30/18

Introduction

CHANGES REHABILITATION LLC. has adopted this Contingency Operations Policy in order to recognize the requirement to comply with the Health Insurance Portability and Accountability Act ("HIPAA"), as amended by the Health Information Technology for Economic and Clinical Health ("HITECH") Act of 2009 (Title XIII of division A and Title IV of division B of the American Recovery and Reinvestment Act "ARRA") and the HIPAA Omnibus Final Rule (Effective Date: March 26, 2013). We acknowledge that full compliance with the HIPAA Final Rule is required by or before September 23, 2013.

CHANGES REHABILITATION LLC.. hereby acknowledges our duty and responsibility to protect the privacy and security of Individually Identifiable Health Information ("IIHI") generally, and Protected Health Information ("PHI") as defined in the HIPAA Regulations, under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under principles of general and professional ethics. We also acknowledge our duty and responsibility to support and facilitate the timely and unimpeded flow of health information for lawful and appropriate purposes.

Scope of Policy

This policy governs Contingency Operations planning and implementation for **CHANGES REHABILITATION LLC..** All personnel of **CHANGES REHABILITATION LLC** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

pdfelement

Assumptions

- **CHANGES REHABILITATION LLC..** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
- **CHANGES REHABILITATION LLC.** must comply with HIPAA and the HIPAA implementing regulations pertaining to contingency operations, in accordance with the requirements at § 164.310(a)(1-2).
- Contingency Operations, for purposes of this policy document, are defined as processes and procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.
- Contingency operations plans and procedures, in combination with other emergency preparedness plans and procedures, shall be documented, analyzed, revised and updated periodically in accordance with other established emergency preparedness and documentation policies and procedures.

Policy Statement

- It is the Policy of **CHANGES REHABILITATION LLC.** to be fully prepared to protect individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA), during emergencies and contingency operations.
- Responsibilities for planning and executing contingency operations shall reside with the Director of IT who shall prepare, analyze, test, and update plans for contingency operations on a periodic basis.
- The primary purpose of our contingency operations procedures is to allow our organization to restore lost data in the event of an emergency.
- It is the Policy of **CHANGES REHABILITATION LLC.** to fully document all contingency operations plans and procedures, in accordance with our Documentation Policy.

Procedures

- See Information Technology Procedure IT08.

- ❑ See Matrix Resource Manual.

Remove Watermark Now

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **CHANGES REHABILITATION LLC.**' s Sanction Policy.

pdfelement

Remove Watermark Now

HIPAA39-Facility Security Policy
Updated: 7/30/18

Introduction

CHANGES REHABILITATION LLC.. has adopted this Facility Security Policy in order to recognize the requirement to comply with the Health Insurance Portability and Accountability Act ("HIPAA"), as amended by the Health Information Technology for Economic and Clinical Health ("HITECH") Act of 2009 (Title XIII of division A and Title IV of division B of the American Recovery and Reinvestment Act "ARRA") and the HIPAA Omnibus Final Rule
(Effective Date: March 26, 2013). We acknowledge that full compliance with the HIPAA Final Rule is required by or before September 23, 2013.

CHANGES REHABILITATION LLC. hereby acknowledges our duty and responsibility to protect the privacy and security of Individually Identifiable Health Information ("IIHI") generally, and Protected Health Information ("PHI") as defined in the HIPAA Regulations, under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under principles of general and professional ethics. We also acknowledge our duty and responsibility to support and facilitate the timely and unimpeded flow of health information for lawful and appropriate purposes.

Scope of Policy

This policy governs Facility Security for **CHANGES REHABILITATION LLC..** All personnel of **CHANGES REHABILITATION LLC.** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

Assumptions

- **CHANGES REHABILITATION LLC.** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
- **CHANGES REHABILITATION LLC.** must comply with HIPAA and the HIPAA implementing regulations pertaining to facility security, in accordance with the requirements at § 164.310(a)(1-2).
- In addition to other technical and administrative safeguards, strong facility security is an essential element of our efforts to provide protection for individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).

Policy Statement

- It is the Policy of **CHANGES REHABILITATION LLC.**to provide strong facility security, in addition to other technical and administrative safeguards, in order to provide protection for individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).
- It is the Policy of **CHANGES REHABILITATION LLC.** to fully document all facility security-related activities and efforts, in accordance with our Documentation Policy and our Maintenance Records Policy.

Procedures

- Primary responsibility for facility security is hereby assigned to the Facility Administrator, who shall analyze the security of our facility and implement devices, tools and techniques to strengthen our facility to a reasonable level, to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.
- The analyses of our facility security should include, but are not limited to, the following factors:
  - Windows and doors
  - Roofs and the potential for roof access
  - Locks and keys

Remove Watermark Now

- Electronic access control systems
- Video cameras and video surveillance systems
- Electronic alarms and related systems
- Employee, partner, vendor and guest access
- Vehicle parking security
- Routine and non-routine deliveries

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **CHANGES REHABILITATION LLC.**' s Sanction Policy.

pdfelement

Remove Watermark Now

HIPAA40-Access Control and Validation Policy
Updated: 7/30/18

Introduction

CHANGES REHABILITATION LLC. has adopted this Access Control and Validation Policy in order to recognize the requirement to comply with the Health Insurance Portability and Accountability Act ("HIPAA"), as amended by the Health Information Technology for Economic and Clinical Health ("HITECH") Act of 2009 (Title XIII of division A and Title IV of division B of the American Recovery and Reinvestment Act "ARRA") and the HIPAA Omnibus Final Rule (Effective Date: March 26, 2013). We acknowledge that full compliance with the HIPAA Final Rule is required by or before September 23, 2013.

CHANGES REHABILITATION LLC. hereby acknowledges our duty and responsibility to protect the privacy and security of Individually Identifiable Health Information ("IIHI") generally, and Protected Health Information ("PHI") as defined in the HIPAA Regulations, under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under principles of general and professional ethics. We also acknowledge our duty and responsibility to support and facilitate the timely and unimpeded flow of health information for lawful and appropriate purposes.

Scope of Policy

This policy governs Access Control and Validation for **CHANGES REHABILITATION LLC.** All personnel of **CHANGES REHABILITATION LLC.** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

pdfelement

Assumptions

- **CHANGES REHABILITATION LLC.** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
- **CHANGES REHABILITATION LLC.** must comply with HIPAA and the HIPAA implementing regulations pertaining to access control and validation, in accordance with the requirements at § 164.310(a)(1-2).
- Access control and validation procedures are designed to control and validate individual access to facilities based on role or function; including visitor control, and access control for software testing and revision.
- Strong access control and validation procedures are an essential element of protecting individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).

Policy Statement

- It is the Policy of **CHANGES REHABILITATION LLC.** to implement and support strong and ongoing access control and validation procedures, in full compliance with all the requirements of HIPAA.
- It is the Policy of **CHANGES REHABILITATION LLC.**to fully document access control and validation procedures, in accordance with our Documentation Policy.

Procedures

- Responsibility for developing, testing, analyzing, and periodically updating access control and validation procedures shall reside with the Director of IT.
- The development and implementation of specific access control and validation procedures shall be conducted in accordance with guidance and information provided by the National Institute of Standards and Technology ("NIST"), or other information technology "best practices".
- Secured and limited access to physical space where Information Technology information is stored.
- Annual Audit.

Compliance and Enforcement

Remove Watermark Now

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **CHANGES REHABILITATION LLC.**'s Sanction Policy.

pdfelement

Remove Watermark Now

HIPAA41-Facility Security Maintenance Records Policy
Updated: 7/30/18

Introduction

CHANGES REHABILITATION LLC. has adopted this Facility Security Maintenance Records Policy in order to recognize the requirement to comply with the Health Insurance Portability and Accountability Act ("HIPAA"), as amended by the Health Information Technology for Economic and Clinical Health ("HITECH") Act of 2009 (Title XIII of division A and Title IV of division B of the American Recovery and Reinvestment Act "ARRA") and the HIPAA Omnibus Final Rule (Effective Date: March 26, 2013). We acknowledge that full compliance with the HIPAA Final Rule is required by or before September 23, 2013.

CHANGES REHABILITATION LLC. hereby acknowledges our duty and responsibility to protect the privacy and security of Individually Identifiable Health Information ("IIHI") generally, and Protected Health Information ("PHI") as defined in the HIPAA Regulations, under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under principles of general and professional ethics. We also acknowledge our duty and responsibility to support and facilitate the timely and unimpeded flow of health information for lawful and appropriate purposes.

Scope of Policy

This policy governs the disposition of records pertaining to maintenance of the physical security of **CHANGES REHABILITATION LLC.**'s facilities. All personnel of **CHANGES REHABILITATION LLC.** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

pdfelement

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

Assumptions

- **CHANGES REHABILITATION LLC..** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
- **CHANGES REHABILITATION LLC.** must comply with HIPAA and the HIPAA implementing regulations pertaining to facility security maintenance records, in accordance with the requirements at § 164.310(a)(1-2).

Policy Statement

- It is the Policy of **CHANGES REHABILITATION LLC.** to create and maintain complete facility security maintenance records, in full compliance with all the requirements of HIPAA.
- Facility security maintenance records are created to document repairs and changes to physical elements of a facility related to security, as detailed in our Facility Security Plan.
- It is the Policy of **CHANGES REHABILITATION LLC.**to fully document facility security maintenance records-related activities and efforts, in accordance with our Documentation Policy.
- Responsibility for the creation and updating of facility security maintenance records is hereby assigned to the Facility Administrator, who shall establish procedures for maintaining such records in appropriate form.

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **CHANGES REHABILITATION LLC.**
s Sanction Policy.

Remove Watermark Now

HIPAA42-Workstation Use Policy
Updated: 7/30/18

Introduction

CHANGES REHABILITATION LLC. has adopted this Workstation Use Policy in order to recognize the requirement to comply with the Health Insurance Portability and Accountability Act ("HIPAA"), as amended by the Health Information Technology for Economic and Clinical Health ("HITECH") Act of 2009 (Title XIII of division A and Title IV of division B of the American Recovery and Reinvestment Act "ARRA") and the HIPAA Omnibus Final Rule (Effective Date: March 26, 2013). We acknowledge that full compliance with the HIPAA Final Rule is required by or before September 23, 2013.

CHANGES REHABILITATION LLC. hereby acknowledges our duty and responsibility to protect the privacy and security of Individually Identifiable Health Information ("IIHI") generally, and Protected Health Information ("PHI") as defined in the HIPAA Regulations, under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under principles of general and professional ethics. We also acknowledge our duty and responsibility to support and facilitate the timely and unimpeded flow of health information for lawful and appropriate purposes.

Scope of Policy

This policy governs Information Workstation Use for **CHANGES REHABILITATION LLC.**. All personnel of **CHANGES REHABILITATION LLC.** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

pdfelement

Assumptions

- ❑ **CHANGES REHABILITATION LLC..** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
- ❑ **CHANGES REHABILITATION LLC.** must comply with HIPAA and the HIPAA implementing regulations pertaining to workstation use, in accordance with the requirements at § 164.310(b) and § 164.310(c).
- ❑ The establishment and implementation of an effective workstation use policy is a crucial element in our overall objective of providing reasonable protections for individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).

Policy Statement

- ❑ It is the Policy of **CHANGES REHABILITATION LLC.** to configure, operate, and maintain our information workstations in full compliance with all the requirements of HIPAA.
- ❑ Our objective in these efforts is to providing reasonable protections for individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).
- ❑ Specific procedures shall be developed to specify the proper functions, procedures, and appropriate environments of workstations that access individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).
- ❑ It is the Policy of **CHANGES REHABILITATION LLC.** to fully document all workstation use-related activities and efforts, in accordance with our Documentation Policy and the requirements of HIPAA.

Procedures

- ❑ Responsibility for the development and implementation of this workstation use policy, and any procedures associated with it, shall reside with the Director of IT, who shall ensure that this policy is maintained, updated as necessary, and implemented fully throughout our organization.
- ❑ Achieve, Matrix and Clinical software are set to time out after 30 minutes for all employees.

- All workstations have a screen saver installed that activates after 5 minutes.
- See Information Technology policies IT00001, IT00005 and IT00007.
- Annual Audit.

Remove Watermark Now

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **CHANGES REHABILITATION LLC.** s Sanction Policy.

pdfelement

Remove Watermark Now

HIPAA43-Workstation Security Policy
Updated: 7/30/18

Introduction

CHANGES REHABILITATION LLC. has adopted this Workstation Security Policy in order to recognize the requirement to comply with the Health Insurance Portability and Accountability Act ("HIPAA"), as amended by the Health Information Technology for Economic and Clinical Health ("HITECH") Act of 2009 (Title XIII of division A and Title IV of division B of the American Recovery and Reinvestment Act "ARRA") and the HIPAA Omnibus Final Rule (Effective Date: March 26, 2013). We acknowledge that full compliance with the HIPAA Final Rule is required by or before September 23, 2013.

CHANGES REHABILITATION LLC. hereby acknowledges our duty and responsibility to protect the privacy and security of Individually Identifiable Health Information ("IIHI") generally, and Protected Health Information ("PHI") as defined in the HIPAA Regulations, under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under principles of general and professional ethics. We also acknowledge our duty and responsibility to support and facilitate the timely and unimpeded flow of health information for lawful and appropriate purposes.

Scope of Policy

This policy governs Workstation Security for **CHANGES REHABILITATION LLC.** All personnel of **CHANGES REHABILITATION LLC.** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

pdfelement

Assumptions

- **CHANGES REHABILITATION LLC.** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
- **CHANGES REHABILITATION LLC.**must comply with HIPAA and the HIPAA implementing regulations pertaining to workstation use, in accordance with the requirements at § 164.310(b) and § 164.310(c).
- The establishment and implementation of an effective workstation security policy is a crucial element in our overall objective or providing reasonable protections for individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).

Policy Statement

- It is the Policy of **CHANGES REHABILITATION LLC.**to establish and maintain this workstation security policy in full compliance with all the requirements of HIPAA.
- Responsibility for the development and implementation of this workstation security policy, and any procedures associated with it, shall reside with the Director of IT, who shall ensure that this policy is maintained, updated as necessary, and implemented fully throughout our organization.
- Specific procedures shall be developed to implement physical safeguards for all workstations that access individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA) to restrict access to authorized users only.
- It is the Policy of **CHANGES REHABILITATION LLC.** to fully document all workstation use-related activities and efforts, in accordance with our Documentation Policy.

Procedures

- Achieve, Casamba and Clinical software are set to time out after 30 minutes for all employees.
- See Information Technology Policies IT00001, IT00005 and IT00007.

Compliance and Enforcement

Remove Watermark Now

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **CHANGES REHABILITATION LLC.**
s Sanction Policy.

pdfelement

Remove Watermark Now

HIPAA44-Media Disposal Policy
Updated: 7/30/18

Introduction

CHANGES REHABILITATION LLC. has adopted this Media Disposal Policy in order to recognize the requirement to comply with the Health Insurance Portability and Accountability Act ("HIPAA"), as amended by the Health Information Technology for Economic and Clinical Health ("HITECH") Act of 2009 (Title XIII of division A and Title IV of division B of the American Recovery and Reinvestment Act "ARRA") and the HIPAA Omnibus Final Rule
(Effective Date: March 26, 2013). We acknowledge that full compliance with the HIPAA Final Rule is required by or before September 23, 2013.

CHANGES REHABILITATION LLC. hereby acknowledges our duty and responsibility to protect the privacy and security of Individually Identifiable Health Information ("IIHI") generally, and Protected Health Information ("PHI") as defined in the HIPAA Regulations, under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under principles of general and professional ethics. We also acknowledge our duty and responsibility to support and facilitate the timely and unimpeded flow of health information for lawful and appropriate purposes.

Scope of Policy

This policy governs Media Disposal for **CHANGES REHABILITATION LLC..** All personnel of **CHANGES REHABILITATION LLC..** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

pdfelement

Assumptions

- **CHANGES REHABILITATION LLC.** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
- **CHANGES REHABILITATION LLC.**must comply with HIPAA and the HIPAA implementing regulations pertaining to media disposal and disposition, in accordance with the requirements at § 164.310(d)(1-2).
- Media containing individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA), must be completely erased, properly encrypted, or totally destroyed in its final disposition, or the data residing on such media is subject to recovery and subsequent misuse or theft.

Policy Statement

- It is the Policy of **CHANGES REHABILITATION LLC.** to dispose of all media containing individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA), in full compliance with all the requirements of HIPAA.
- Responsibility for proper media disposal and disposition shall reside with the Director of IT, who shall develop procedures to ensure the proper disposition of all such media.
- It is the Policy of **CHANGES REHABILITATION LLC.** to fully document all media disposal-related activities and efforts, in accordance with our Documentation Policy.

Procedures

- See Information Technology policy IT00011.
- See Information Technology procedure IT04.
- **CHANGES REHABILITATION LLC.** receives a certificate after media is destroyed.

Compliance and Enforcement

Remove Watermark Now

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **CHANGES REHABILITATION LLC.**'s Sanction Policy.

pdfelement

Remove Watermark Now

HIPAA45-Media Re-Use Policy
Updated: 7/30/18

Introduction

CHANGES REHABILITATION LLC. has adopted this Media Re-Use Policy in order to recognize the requirement to comply with the Health Insurance Portability and Accountability Act ("HIPAA"), as amended by the Health Information Technology for Economic and Clinical Health ("HITECH") Act of 2009 (Title XIII of division A and Title IV of division B of the American Recovery and Reinvestment Act "ARRA") and the HIPAA Omnibus Final Rule
(Effective Date: March 26, 2013). We acknowledge that full compliance with the HIPAA Final Rule is required by or before September 23, 2013.

CHANGES REHABILITATION LLC.. hereby acknowledges our duty and responsibility to protect the privacy and security of Individually Identifiable Health Information ("IIHI") generally, and Protected Health Information ("PHI") as defined in the HIPAA Regulations, under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under principles of general and professional ethics. We also acknowledge our duty and responsibility to support and facilitate the timely and unimpeded flow of health information for lawful and appropriate purposes.

Scope of Policy

This policy governs the Re-Use of Information Storage Media for **CHANGES REHABILITATION LLC.** All personnel of **CHANGES REHABILITATION LLC..** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce
.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

pdfelement

Assumptions

- **CHANGES REHABILITATION LLC.** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
- **CHANGES REHABILITATION LLC.** must comply with HIPAA and the HIPAA implementing regulations pertaining to media disposal and disposition, in accordance with the requirements at § 164.310(d)(1-2).
- Media containing individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA), must be completely erased or sanitized ("wiped") before any re-use of such media may take place, or the data residing on such media is subject to corruption, compromise, or loss.

Policy Statement

- It is the Policy of **CHANGES REHABILITATION LLC.**to properly erase and or sanitize ("wipe") all media containing individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA), before any media may be re-used, unless being utilized by the same job function.
- Responsibility for proper media re-use shall reside with the Director of IT, who shall develop procedures to ensure the proper disposition of all such media before any re-use.
- It is the Policy of **CHANGES REHABILITATION LLC.**to fully document media re-use and disposition-related activities and efforts, in accordance with our Documentation Policy.

Procedures

- See Information Technology Policy IT00011.
- See Information Technology Procedure IT04.

Compliance and Enforcement

Remove Watermark Now

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **CHANGES REHABILITATION LLC.**
s Sanction Policy.

pdfelement

Remove Watermark Now

HIPAA46-Hardware and Media Accountability Policy
Updated: 7/30/18

Introduction

CHANGES REHABILITATION LLC. has adopted this Hardware and Media Accountability Policy in order to recognize the requirement to comply with the Health Insurance Portability and Accountability Act ("HIPAA"), as amended by the Health Information Technology for Economic and Clinical Health ("HITECH") Act of 2009 (Title XIII of division A and Title IV of division B of the American Recovery and Reinvestment Act "ARRA") and the HIPAA Omnibus Final Rule (Effective Date: March 26, 2013). We acknowledge that full compliance with the HIPAA Final Rule is required by or before September 23, 2013.

CHANGES REHABILITATION LLC.hereby acknowledges our duty and responsibility to protect the privacy and security of Individually Identifiable Health Information ("IIHI") generally, and Protected Health Information ("PHI") as defined in the HIPAA Regulations, under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under principles of general and professional ethics. We also acknowledge our duty and responsibility to support and facilitate the timely and unimpeded flow of health information for lawful and appropriate purposes.

Scope of Policy

This policy governs the Accountability of Information Systems Hardware and Media for **CHANGES REHABILITATION LLC.** All personnel of **CHANGES REHABILITATION LLC.** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

pdfelement

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

Assumptions

- **CHANGES REHABILITATION LLC.** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
- **CHANGES REHABILITATION LLC.** must comply with HIPAA and the HIPAA implementing regulations, in accordance with the requirements at § 164.310(d)(1-2).
- Proper protection of individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA), requires that we maintain records of the movements of hardware and electronic media, and any person responsible therefore.

Policy Statement

- It is the Policy of **CHANGES REHABILITATION LLC.** to maintain records of the movements of hardware and electronic media, and any person responsible therefore, in full compliance with all the requirements of HIPAA.
- Responsibility for the development and implementation of this hardware and media accountability policy, and any procedures associated with it, shall reside with the Director of IT, who shall ensure that this policy is maintained, updated as necessary, and implemented fully throughout our organization.
- Specific procedures shall be developed to ensure that we maintain records of the movements of hardware and electronic media, and any person responsible therefore.
- It is the Policy of **CHANGES REHABILITATION LLC.**to fully document all hardware and media accountability- related activities and efforts, in accordance with our Documentation Policy.

Procedures

- See Information Technology Procedure IT10.

Compliance and Enforcement

Remove Watermark Now

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **CHANGES REHABILITATION LLC.**'s Sanction Policy.

pdfelement

Remove Watermark Now

HIPAA47-Data Backup and Storage Policy
Updated: 7/30/18

Introduction

CHANGES REHABILITATION LLC. has adopted this Data Backup and Storage Policy in order to recognize the requirement to comply with the Health Insurance Portability and Accountability Act ("HIPAA"), as amended by the Health Information Technology for Economic and Clinical Health ("HITECH") Act of 2009 (Title XIII of division A and Title IV of division B of the American Recovery and Reinvestment Act "ARRA") and the HIPAA Omnibus Final Rule (Effective Date: March 26, 2013). We acknowledge that full compliance with the HIPAA Final Rule is required by or before September 23, 2013.

CHANGES REHABILITATION LLC. hereby acknowledges our duty and responsibility to protect the privacy and security of Individually Identifiable Health Information ("IIHI") generally, and Protected Health Information ("PHI") as defined in the HIPAA Regulations, under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under principles of general and professional ethics. We also acknowledge our duty and responsibility to support and facilitate the timely and unimpeded flow of health information for lawful and appropriate purposes.

Scope of Policy

This policy governs Data Backup and Storage for **CHANGES REHABILITATION LLC.**. All personnel of **CHANGES REHABILITATION LLC..** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

pdfelement

Assumptions

- ❑ **CHANGES REHABILITATION LLC.** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
  - ❑ **CHANGES REHABILITATION LLC.** must comply with HIPAA and the HIPAA implementing regulations pertaining to data backup and storage, in accordance with the requirements at § 164.310(d)(1-2) and § 164.308(a)(7).
- ❑ The ability to create and maintain retrievable, exact copies of individually identifiable health information generally, and electronic protected health information specifically, is a critical element of our business operations and our ability to respond to unexpected negative events.
- ❑ The storage of data backups in a separate location, removed from our normal business operations ("offsite") is an essential element of any successful data backup plan.
- ❑ Timely access to health information is crucial to providing high quality health care, and to our business operations.
- ❑ Physicians and others must have immediate, around-the-clock access to patient information.
- ❑ No existing media are absolutely guaranteed to provide long-term storage without loss or corruption of data.
- ❑ A number of risks to health information exist, such as power spikes or outages, fire, flood, or other natural disaster, viruses, hackers, and improper acts by employees and others.

Policy Statement

- ❑ It is the Policy of **CHANGES REHABILITATION LLC.** to create retrievable, exact copies of electronic protected health information, when needed, before any movement or maintenance of data processing equipment that could result in the loss or compromise of electronic protected health information.
- ❑ The Director of IT is responsible for performing appropriate backups on **CHANGES REHABILITATION LLC**.'s network, including shared drives containing application data, patient information, financial data, and crucial system information.

Procedures

Remove Watermark Now

- **CHANGES REHABILITATION LLC..** will back up all such data as necessary, per Unitrend's programmed standards, before any movement or maintenance of data processing equipment that could result in the loss or compromise of electronic protected health information..
- The Director of IT or his or her designee will, no later than 0900 the next day, place the backup media into the media vault located in Location of Backup Vault or Facility.
- The media vault meets fire and disaster standards for media and will be kept locked at all times. Only The Director of IT, the system administrator, and their designees have access to the media vault.
- In the event that the secured media vault is not available or properly functioning, The Director of IT, the system administrator, or their designees will remove backup media to a secured offsite location until the media vault becomes available.
- Any errors will be acted upon immediately. Responsible personnel will use contract technical support as needed to resolve problems and ensure the validity of backup data.
- Responsible personnel will clean the backup unit(s) according to the manufacturer's recommended guidelines, currently once per week.
- The Director of IT will ensure replacement of media according to manufacturer's recommended guidelines, currently annually.
- The Director of IT is responsible for testing the validity of backup data and the ability to restore data in the event of a computer system problem, failure, or other disaster at least monthly(or specify other timeframe), and more often if necessary to ensure data integrity, availability, and confidentiality.
- Successful restore functions must be logged in the network log. Any problems identified during the restore function must be acted on immediately and no later than the same business day that they occur. Responsible personnel will use contract technical support as needed to resolve problems and ensure the validity of backup data.
- All personnel who detect or suspect a data backup problem should immediately report the same to the Director of IT. Such personnel should follow up immediate notification with a written memorandum that includes the following information:
    - Narrative of the data backup problem.
    - How long the problem has existed.
    - Suggested solutions.
- See Information Technology Procedure IT08.

pdfelement

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **CHANGES REHABILITATION LLC.**'s Sanction Policy.

Remove Watermark Now

HIPAA48-Unique User I.D. Policy
Updated: 7/30/18

Introduction

CHANGES REHABILITATION LLC.has adopted this Unique User I.D. Policy in order to recognize the requirement to comply with the Health Insurance Portability and Accountability Act ("HIPAA"), as amended by the Health Information Technology for Economic and Clinical Health ("HITECH") Act of 2009 (Title XIII of division A and Title IV of division B of the American Recovery and Reinvestment Act "ARRA") and the HIPAA Omnibus Final Rule (Effective Date: March 26, 2013). We acknowledge that full compliance with the HIPAA Final Rule is required by or before September 23, 2013.

CHANGES REHABILITATION LLC.hereby acknowledges our duty and responsibility to protect the privacy and security of Individually Identifiable Health Information ("IIHI") generally, and Protected Health Information ("PHI") as defined in the HIPAA Regulations, under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under principles of general and professional ethics. We also acknowledge our duty and responsibility to support and facilitate the timely and unimpeded flow of health information for lawful and appropriate purposes.

Scope of Policy

This policy governs the issuance, maintenance, and security of Unique User I.D.'s for access to **CHANGES REHABILITATION LLC.**'s information systems. All personnel of **CHANGES REHABILITATION LLC.** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

pdfelement

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

Assumptions

- **CHANGES REHABILITATION LLC.** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
- **CHANGES REHABILITATION LLC.** must comply with HIPAA and the HIPAA implementing regulations pertaining to the use of unique user I.D.'s, in accordance with the requirements at § 164.306, and § 164.312(a)(1).
- The use of unique user I.D.'s is an essential element in our overall effort to protect individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).

Policy Statement

- It is the Policy of **CHANGES REHABILITATION LLC.**to exclusively use unique user I.D.'s for all information system access and activities, in full compliance with all the requirements of HIPAA.
- Responsibility for the development and implementation of this unique user I.D. policy, and any procedures associated with it, shall reside with the Director of IT, who shall ensure that access to all our information systems and data is accomplished exclusively through the use of unique user I.D.'s.
- Nothing in this policy shall limit the use of additional security measures, including login and access measures, that may further enhance the security and protection we provide to individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).
- It is the Policy of **CHANGES REHABILITATION LLC.** to fully document all unique user I.D.-related activities and efforts, in accordance with our Documentation Policy.

Procedures

- See Information Technology Procedure IT17.
- See Information Technology Policy IT00002.

Compliance and Enforcement

Remove Watermark Now

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **CHANGES REHABILITATION LLC.**'s Sanction Policy.

pdfelement

Remove Watermark Now

HIPAA49-Emergency Access Policy
Updated: 7/30/18

Introduction

CHANGES REHABILITATION LLC. has adopted this Emergency Access Policy in order to recognize the requirement to comply with the Health Insurance Portability and Accountability Act ("HIPAA"), as amended by the Health Information Technology for Economic and Clinical Health ("HITECH") Act of 2009 (Title XIII of division A and Title IV of division B of the American Recovery and Reinvestment Act "ARRA") and the HIPAA Omnibus Final Rule (Effective Date: March 26, 2013). We acknowledge that full compliance with the HIPAA Final Rule is required by or before September 23, 2013.

CHANGES REHABILITATION LLC.. hereby acknowledges our duty and responsibility to protect the privacy and security of Individually Identifiable Health Information ("IIHI") generally, and Protected Health Information ("PHI") as defined in the HIPAA Regulations, under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under principles of general and professional ethics. We also acknowledge our duty and responsibility to support and facilitate the timely and unimpeded flow of health information for lawful and appropriate purposes.

Scope of Policy

This policy governs Access to Protected Health Information during emergencies for **CHANGES REHABILITATION LLC.** All personnel of **CHANGES REHABILITATION LLC**. must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

pdfelement

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

Assumptions

- **CHANGES REHABILITATION LLC.** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
- **CHANGES REHABILITATION LLC.** must comply with HIPAA and the HIPAA implementing regulations pertaining to emergency access procedures, in accordance with the requirements at § 164.104, § 164.306, and § 164.312(a)(1).
- The establishment of emergency access procedures further strengthens the protections we offer to individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).

Policy Statement

- It is the Policy of **CHANGES REHABILITATION LLC.** to establish and maintain this encryption and decryption policy in full compliance with all the requirements of HIPAA.
- Responsibility for these emergency access procedures apply to access to individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).
- Responsibility for the development and implementation of our emergency access procedures as it relates to digital data and the internet shall reside with the Director of IT, who shall ensure that these procedures are maintained, updated as necessary, and implemented fully throughout our organization.
- Specific procedures shall be developed to ensure that authorized workforce members can access individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA) during emergencies.
- These Emergency Access Procedures shall be developed and implemented in combination with our emergency preparedness and response plans.
- It is the Policy of **CHANGES REHABILITATION LLC..** to fully document our emergency access procedures development and implementation, in accordance with our Documentation Policy and the requirements of HIPAA.

Remove Watermark Now

Procedures

- ❑ See Matrix Resource Manual for downtime procedure.

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **CHANGES REHABILITATION LLC.**' s Sanction Policy.

pdfelement

Remove Watermark Now

HIPAA50-Automatic Log-Off Policy
Updated: 7/30/18

Introduction

CHANGES REHABILITATION LLC.. has adopted this Automatic Log-Off Policy in order to recognize the requirement to comply with the Health Insurance Portability and Accountability Act ("HIPAA"), as amended by the Health Information Technology for Economic and Clinical Health ("HITECH") Act of 2009 (Title XIII of division A and Title IV of division B of the American Recovery and Reinvestment Act "ARRA") and the HIPAA Omnibus Final Rule (Effective Date: March 26, 2013). We acknowledge that full compliance with the HIPAA Final Rule is required by or before September 23, 2013.

CHANGES REHABILITATION LLC. hereby acknowledges our duty and responsibility to protect the privacy and security of Individually Identifiable Health Information ("IIHI") generally, and Protected Health Information ("PHI") as defined in the HIPAA Regulations, under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under principles of general and professional ethics. We also acknowledge our duty and responsibility to support and facilitate the timely and unimpeded flow of health information for lawful and appropriate purposes.

Scope of Policy

This policy governs the implementation of Automatic Log-Offs for **CHANGES REHABILITATION LLC.**'s information systems. All personnel of **CHANGES REHABILITATION LLC.** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

Assumptions

- **CHANGES REHABILITATION LLC.** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
- **CHANGES REHABILITATION LLC..** must comply with HIPAA and the HIPAA implementing regulations pertaining to the use of automatic log-off applications, in accordance with the requirements at § 164.306 and § 164.312(a)(1-2).
- The establishment and implementation of an effective automatic log-off policy is a crucial element in our overall objective or providing reasonable protections for individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).

Policy Statement

- It is the Policy of **CHANGES REHABILITATION LLC.** to always use automatic log-off applications or systems on all workstations and computers, in full compliance with the requirements of HIPAA.
- Responsibility for the development and implementation of this automatic log-off policy, and any procedures associated with it, shall reside with the Director of IT, who shall ensure that this policy is maintained, updated as necessary, and implemented fully throughout our organization.
- Specific procedures shall be developed to specify the proper functions and procedures of our automatic log-off systems on all computers and workstations that access individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).
- It is the Policy of **CHANGES REHABILITATION LLC.** to fully document automatic log-off-related activities and efforts, in accordance with our Documentation Policy.

pdfelement

Remove Watermark Now

Procedure

- Achieve, Casamba and Clinical software is set to time out after 30 minutes for all employees.
- See Information Technology Policies IT00001, IT00005 and IT00007.

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **CHANGES REHABILITATION LLC.**' s Sanction Policy.

pdfelement

Remove Watermark Now

HIPAA51-Encryption and Decryption Policy
Updated: 7/30/18

Introduction

CHANGES REHABILITATION LLC. has adopted this Encryption and Decryption Policy in order to recognize the requirement to comply with the Health Insurance Portability and Accountability Act ("HIPAA"), as amended by the Health Information Technology for Economic and Clinical Health ("HITECH") Act of 2009 (Title XIII of division A and Title IV of division B of the American Recovery and Reinvestment Act "ARRA") and the HIPAA Omnibus Final Rule (Effective Date: March 26, 2013). We acknowledge that full compliance with the HIPAA Final Rule is required by or before September 23, 2013.

CHANGES REHABILITATION LLC. hereby acknowledges our duty and responsibility to protect the privacy and security of Individually Identifiable Health Information ("IIHI") generally, and Protected Health Information ("PHI") as defined in the HIPAA Regulations, under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under principles of general and professional ethics. We also acknowledge our duty and responsibility to support and facilitate the timely and unimpeded flow of health information for lawful and appropriate purposes.

Scope of Policy

This policy governs the Encryption and Decryption of Protected Health Information for **CHANGES REHABILITATION LLC.** All personnel of **CHANGES REHABILITATION LLC.** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

pdfelement

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

Assumptions

- ❑ **CHANGES REHABILITATION LLC.** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
- ❑ **CHANGES REHABILITATION LLC.** must comply with HIPAA and the HIPAA implementing regulations pertaining to encryption and decryption, in accordance with the requirements at § 164.312(a)(1-2).
- ❑ The establishment and implementation of an effective encryption and decryption policy is a crucial element in our overall objective or providing reasonable protections for individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).

Policy Statement

- ❑ It is the Policy of **CHANGES REHABILITATION LLC..** to establish and maintain this encryption and decryption policy in full compliance with all the requirements of HIPAA.
- ❑ Responsibility for the development and implementation of this encryption and decryption policy, and any procedures associated with it, shall reside with the Director of IT, who shall ensure that this policy is maintained, updated as necessary, and implemented fully throughout our organization.
- ❑ Specific procedures shall be developed to specify the proper usage and application of encryption and decryption for all computers and workstations that access individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).
- ❑ It is the Policy of **CHANGES REHABILITATION LLC.** to fully document all encryption and decryption-related activities and efforts, in accordance with our Documentation Policy.
- ❑ It is the policy of **CHANGES REHABILITATION LLC.**. to encrypt patient data via the clinical software that we use. ❑ It is the policy of **CHANGES REHABILITATION LLC.**. to encrypt patient data on the server .

Procedures

- ❑ All software using PHI must utilize 128bit encryption.

- All web based applications using PHI must utilize HTTPS or SFTP as communication protocol.

Remove Watermark Now

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **CHANGES REHABILITATION LLC ..**'s Sanction Policy.

pdfelement

Remove Watermark Now

HIPAA52-Audit Controls Policy
Updated: 7/30/18

Introduction

CHANGES REHABILITATION LLC. has adopted this Audit Controls Policy in order to recognize the requirement to comply with the Health Insurance Portability and Accountability Act ("HIPAA"), as amended by the Health Information Technology for Economic and Clinical Health ("HITECH") Act of 2009 (Title XIII of division A and Title IV of division B of the American Recovery and Reinvestment Act "ARRA") and the HIPAA Omnibus Final Rule
(Effective Date: March 26, 2013). We acknowledge that full compliance with the HIPAA Final Rule is required by or before September 23, 2013.

CHANGES REHABILITATION LLC.hereby acknowledges our duty and responsibility to protect the privacy and security of Individually Identifiable Health Information ("IIHI") generally, and Protected Health Information ("PHI") as defined in the HIPAA Regulations, under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under principles of general and professional ethics. We also acknowledge our duty and responsibility to support and facilitate the timely and unimpeded flow of health information for lawful and appropriate purposes.

Scope of Policy

This policy governs Audit Controls for **CHANGES REHABILITATION LLC.** All personnel of **CHANGES REHABILITATION LLC.** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

pdfelement

Assumptions

- **CHANGES REHABILITATION LLC.** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
- **CHANGES REHABILITATION LLC.** must comply with HIPAA and the HIPAA implementing regulations pertaining to audit controls, in accordance with the requirements at § 164.312(b).
- The establishment and implementation of an effective audit controls policy is a crucial element in our overall objective or providing reasonable protections for individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).

Policy Statement

- It is the Policy of **CHANGES REHABILITATION LLC.** to establish and maintain appropriate and effective audit controls in full compliance with the requirements of HIPAA.
- Responsibility for the development and implementation of this audit controls policy, and any procedures associated with it, shall reside with the Director of IT, who shall ensure that this policy is maintained, updated as necessary, and implemented fully throughout our organization.
- Specific procedures shall be developed to specify the proper usage and application of audit controls for all computers, workstations, and systems that access individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).
- It is the Policy of **CHANGES REHABILITATION LLC.**to fully document all audit control-related activities and efforts, in accordance with our Documentation Policy.

Procedures

- Annual audit.

Compliance and Enforcement

Remove Watermark Now

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **CHANGES REHABILITATION LLC ..**'s Sanction Policy.

pdfelement

Remove Watermark Now

HIPAA53-Data Integrity Controls Policy
Updated: 7/30/18

Introduction

CHANGES REHABILITATION LLC. has adopted this Data Integrity Controls Policy in order to recognize the requirement to comply with the Health Insurance Portability and Accountability Act ("HIPAA"), as amended by the Health Information Technology for Economic and Clinical Health ("HITECH") Act of 2009 (Title XIII of division A and Title IV of division B of the American Recovery and Reinvestment Act "ARRA") and the HIPAA Omnibus Final Rule (Effective Date: March 26, 2013). We acknowledge that full compliance with the HIPAA Final Rule is required by or before September 23, 2013.

CHANGES REHABILITATION LLC.hereby acknowledges our duty and responsibility to protect the privacy and security of Individually Identifiable Health Information ("IIHI") generally, and Protected Health Information ("PHI") as defined in the HIPAA Regulations, under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under principles of general and professional ethics. We also acknowledge our duty and responsibility to support and facilitate the timely and unimpeded flow of health information for lawful and appropriate purposes.

Scope of Policy

This policy governs Data Integrity Controls for **CHANGES REHABILITATION LLC .** All personnel of **CHANGES REHABILITATION LLC .** must comply with this policy . Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

pdfelement

Assumptions

- **CHANGES REHABILITATION LLC.** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
- **CHANGES REHABILITATION LLC.** must comply with HIPAA and the HIPAA implementing regulations pertaining to data integrity controls, in accordance with the requirements at § 164.312(c)(1-2).
- The purpose of this Integrity Controls Policy is to ensure that electronic Protected Health Information ("PHI" and "ePHI", as defined by HIPAA) has not been altered or destroyed in an unauthorized manner.
- The establishment and implementation of an effective data integrity controls policy is a crucial element in our overall objective or providing reasonable protections for individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).

Policy Statement

- It is the Policy of **CHANGES REHABILITATION LLC.** to establish and maintain appropriate and effective data integrity controls in full compliance with the requirements of HIPAA.
- Responsibility for the development and implementation of this data integrity controls policy, and any procedures associated with it, shall reside with the Director of IT and the Corporate Compliance Officer, who shall ensure that this policy is maintained, updated as necessary, and implemented fully throughout our organization.
- Specific procedures shall be developed to specify the proper usage and application of data integrity controls for all computers, workstations, and systems that access individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).
- It is the Policy of **CHANGES REHABILITATION LLC.** to fully document all data integrity controls-related activities and efforts, in accordance with our Documentation Policy.

Procedures

Remove Watermark Now

- ❑ Corporate Compliance password audit.
- ❑ Achieve/Matrix software, Clinical Ops and email are HTTPS encrypted.
- ❑ See Information Technology policies IT00001 and IT00002.

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **CHANGES REHABILITATION LLC ..**'s Sanction Policy.

pdfelement

Remove Watermark Now

HIPAA54-Person or Entity Authentication Policy
Updated: 7/30/18

Introduction

CHANGES REHABILITATION LLC. has adopted this Person or Entity Authentication Policy in order to recognize the requirement to comply with the Health Insurance Portability and Accountability Act ("HIPAA"), as amended by the Health Information Technology for Economic and Clinical Health ("HITECH") Act of 2009 (Title XIII of division A and Title IV of division B of the American Recovery and Reinvestment Act "ARRA") and the HIPAA Omnibus Final Rule (Effective Date: March 26, 2013). We acknowledge that full compliance with the HIPAA Final Rule is required by or before September 23, 2013.

CHANGES REHABILITATION LLC.. hereby acknowledges our duty and responsibility to protect the privacy and security of Individually Identifiable Health Information ("IIHI") generally, and Protected Health Information ("PHI") as defined in the HIPAA Regulations, under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under principles of general and professional ethics. We also acknowledge our duty and responsibility to support and facilitate the timely and unimpeded flow of health information for lawful and appropriate purposes.

Scope of Policy

This policy governs Authentication of Persons or Entities seeking access to Electronic Protected Health Information in the possession of **CHANGES REHABILITATION LLC.**All personnel of **CHANGES REHABILITATION LLC.** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

pdfelement

Assumptions

- **CHANGES REHABILITATION LLC.**hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
- **CHANGES REHABILITATION LLC.**must comply with HIPAA and the HIPAA implementing regulations pertaining to person or entity authentication, in accordance with the requirements at § 164.312(d).
- The purpose of this Person or Entity Authentication Policy is to ensure that electronic Protected Health Information ("PHI" and "ePHI", as defined by HIPAA) can only be accessed by persons or entities who are in fact who they claim to be, and not imposters.
- The establishment and implementation of an effective Person or Entity Authentication Policy is a crucial element in our overall objective or providing reasonable protections for individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).

Policy Statement

- It is the Policy of **CHANGES REHABILITATION LLC.** to establish and maintain this Person or Entity Authentication Policy in full compliance with all the requirements of HIPAA.
- Responsibility for the development and implementation of this Person or Entity Authentication Policy, and any procedures associated with it, shall reside with the Director of IT, who shall ensure that this policy is maintained, updated as necessary, and implemented fully throughout our organization.
- Specific procedures shall be developed to specify the proper authentication of persons and entities who request access to individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA) on our computers, workstations and systems.
- It is the Policy of **CHANGES REHABILITATION LLC.** to fully document all person or entity-related activities and efforts, in accordance with our Documentation Policy.

Remove Watermark Now

Procedures

- See Information Technology Policies IT00012 and IT00002.

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **CHANGES REHABILITATION LLC**.'s Sanction Policy.

pdfelement

Remove Watermark Now

HIPAA55-Data Transmission Security Policy
Updated: 7/30/18

Introduction

CHANGES REHABILITATION LLC. has adopted this Data Transmission Security Policy in order to recognize the requirement to comply with the Health Insurance Portability and Accountability Act ("HIPAA"), as amended by the Health Information Technology for Economic and Clinical Health ("HITECH") Act of 2009 (Title XIII of division A and Title IV of division B of the American Recovery and Reinvestment Act "ARRA") and the HIPAA Omnibus Final Rule (Effective Date: March 26, 2013). We acknowledge that full compliance with the HIPAA Final Rule is required by or before September 23, 2013.

CHANGES REHABILITATION LLC. hereby acknowledges our duty and responsibility to protect the privacy and security of Individually Identifiable Health Information ("IIHI") generally, and Protected Health Information ("PHI") as defined in the HIPAA Regulations, under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under principles of general and professional ethics. We also acknowledge our duty and responsibility to support and facilitate the timely and unimpeded flow of health information for lawful and appropriate purposes.

Scope of Policy

This policy governs Data Transmission Security for **CHANGES REHABILITATION LLC.** All personnel of **CHANGES REHABILITATION LLC.** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

pdfelement

Assumptions

- ❑ **CHANGES REHABILITATION LLC.** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
- ❑ **CHANGES REHABILITATION LLC.** must comply with HIPAA and the HIPAA implementing regulations pertaining to data transmission security, in accordance with the requirements at § 164.312(e)(1) and § 164.312(e)(2).
- ❑ The purpose of our Data Transmission Security Policy and Procedures is to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.
- ❑ The establishment and implementation of effective Data Transmission Security Procedures is a crucial element in our overall objective or providing reasonable protections for individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).

Policy Statement

- ❑ It is the Policy of **CHANGES REHABILITATION LLC.** to establish and implement technical security measures to guard against unauthorized access to Electronic Protected Health Information that is being transmitted over an electronic communications network, in full compliance with the requirements of HIPAA.
- ❑ Responsibility for the development and implementation of these Data Transmission Security Procedures shall reside with the Director of IT, who shall ensure that these procedures are maintained, updated as necessary, and implemented fully throughout our organization.
- ❑ Specific Data Transmission Security Procedures shall be developed to protect individually identifiable health information, including Electronic Protected Health Information ("EPHI", as defined by HIPAA).
- ❑ It is the Policy of **CHANGES REHABILITATION LLC.** to fully document all Data Transmission Security Procedures, activities, and efforts, in accordance with our Documentation Policy and the requirements of HIPAA.

Remove Watermark Now

Procedures

- **CHANGES REHABILITATION LLC.** incorporates HIPAA email notifications on all outgoing email.
- Achieve/Matrix, Clinical Ops and company email are 128 bit encrypted.
- See Information Technology policy IT00001 and IT00018.

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **CHANGES REHABILITATION LLC.**' s Sanction Policy.

pdfelement

Remove Watermark Now

HIPAA56-Mobile Device Policy
Updated: 7/30/18

Introduction

CHANGES REHABILITATION LLC. has adopted this Mobile Device Policy in order to recognize the requirement to comply with the Health Insurance Portability and Accountability Act ("HIPAA"), as amended by the Health Information Technology for Economic and Clinical Health ("HITECH") Act of 2009 (Title XIII of division A and Title IV of division B of the American Recovery and Reinvestment Act "ARRA") and the HIPAA Omnibus Final Rule
(Effective Date: March 26, 2013). We acknowledge that full compliance with the HIPAA Final Rule is required by or before September 23, 2013.

CHANGES REHABILITATION LLC.hereby acknowledges our duty and responsibility to protect the privacy and security of Individually Identifiable Health Information ("IIHI") generally, and Protected Health Information ("PHI") as defined in the HIPAA Regulations, under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under principles of general and professional ethics. We also acknowledge our duty and responsibility to support and facilitate the timely and unimpeded flow of health information for lawful and appropriate purposes.

Scope of Policy

This policy governs the use of mobile devices that can access, use, transmit, or store Individually Identifiable Health Information ("IIHI"), and Protected Health Information ("PHI") in the custody of **CHANGES REHABILITATION LLC.** All personnel of **CHANGES REHABILITATION LLC.** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

Assumptions

- **CHANGES REHABILITATION LLC.** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA Regulations.
- **CHANGES REHABILITATION LLC.** must comply with HIPAA and the HIPAA implementing regulations, in accordance with the requirements at 45 CFR Parts 160 and 164, as amended.
- Full compliance with HIPAA is mandatory and failure to comply can bring severe sanctions and penalties. Possible sanctions and penalties include, but are not limited to: civil monetary penalties, criminal penalties including prison sentences, and loss of revenue and reputation from negative publicity.
- Full compliance with HIPAA strengthens our ability to meet other compliance obligations, and will support and strengthen our non-HIPAA compliance requirements and efforts.
- Full compliance with HIPAA reduces the overall risk of inappropriate uses and disclosures of Protected Health Information (PHI), and reduces the risk of breaches of confidential health data.
- The requirements of the HIPAA Administrative Simplification Regulations (including the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules) implement sections 1171-1180 of the Social Security Act (the Act), sections 262 and 264 of Public Law 104-191, section 105 of 492 Public Law 110-233, sections 13400-13424 of Public Law 111-5, and section 1104 of Public Law 111-148.

Policy Statement

- It is the Policy of **CHANGES REHABILITATION LLC.**to extend all the privacy and security protections required by HIPAA to Protected Health Information accessed, used, transmitted, and stored on mobile devices operated by members of our workforce.
- It is the Policy of **CHANGES REHABILITATION LLC.** to include privacy and security issues related to mobile devices in our Risk Management process and analysis, to better understand risks inherent in the use of such devices.

- This Policy applies to all electronic computing and communications devices which may be readily carr by an individual and are capable of receiving, processing, or transmitting Protected Health Information, whether directly through download or upload, text entry, photograph or video, from any data source, whether through wireless, network or direct connection to a computer, other Mobile Device, or any equipment capable of recording, storing or transmitting digital information (such as copiers or medical devices). Mobile Devices include, but are not limited to smartphones, digital music players, hand-held computers, laptop computers, tablet computers, and personal digital assistants (PDAs).
- This Policy applies to personally-owned Mobile Devices as well as Mobile Devices owned or leased by, and provided by **CHANGES REHABILITATION LLC.**
- Mobile Devices which cannot be or have not been configured to comply with this Policy are prohibited.
- It is the Policy of **CHANGES REHABILITATION LLC.**to limit the access, use, transmittal, and storage of Protected Health Information exclusively to those mobile devices that can be configured and operated to deliver privacy and security comparable to the non-mobile data processing systems and devices that we operate.
- It is the Policy of **CHANGES REHABILITATION LLC.**to limit the access, use, transmittal and storage of Protected Health Information on mobile devices to the Minimum Necessary, as that term is defined in the HIPAA Regulations.
- It is the Policy of **CHANGES REHABILITATION LLC.** to train workforce members on the safe and secure usage of mobile devices that are utilized to access, use, transmit, or store Protected Health Information
- It is the Policy of **CHANGES REHABILITATION LLC.**to fully document all mobile device-related activities which involve Protected Health Information, in accordance with our Documentation Policy and the requirements of HIPAA.

Procedures

- No Mobile Device may be used for any purpose or activity involving information subject to this Policy without prior registration of the device and written authorization by the Director of IT. Authorization will be given only for uses of Mobile Devices confirmed to have been configured to be compliant with this Policy.
- Any access, use, transmittal or storage of Protected Health Information subject to this Policy by a Mobile Device, and any use of a Mobile Device in any **CHANGES REHABILITATION LLC.** facility or office, including an authorized home office or remote site, must be in compliance with all **CHANGES REHABILITATION LLC.** policies at all times.
- Authorization to use a Mobile Device may be suspended at any time:
  - If the User fails or refuses to comply with this Policy;
  - In order to avoid, prevent or mitigate the consequences of a violation of this Policy;
  - In connection with the investigation of a possible or proven security breach, security incident, or violation of **CHANGES REHABILITATION LLC.**'s policies;
  - In order to protect life, health, privacy, reputational or financial interests; to protect any assets, information, reputational or financial interests of **CHANGES REHABILITATION LLC.**
  - Upon request of a supervisor or department head in which the User works; or
  - Upon the direction of the Corporate Compliance Officer or Director of IT.
- Authorization to use a Mobile Device terminates:
  - Automatically upon the termination of a User's status as a member of **CHANGES REHABILITATION LLC.**'s workforce;
  - Upon a change in the User's role as a member of **CHANGES REHABILITATION LLC.**'s Workforce, unless continued authorization is authorized in writing.
  - If it is determined that the User violated this or any other **CHANGES REHABILITATION LLC.** policy, in accordance with **CHANGES REHABILITATION LLC.**'s Sanction policy.
- The use of a Mobile Device without authorization, while authorization is suspended, or after authorization has been terminated is a violation of this Policy.
- At any time, any Mobile Device may be subject to audit to ensure compliance with this and other **CHANGES REHABILITATION LLC.** policies. Any User receiving such a request shall transfer possession of the Mobile Device to IT Department/Corporate Compliance/ Management. at once, unless a later transfer date and time is indicated in the request, and shall not delete or modify any information subject to this Policy which is stored on the Mobile Device after receiving the request.
- See Information Technology Policy IT00018.

Compliance and Enforcement

All **CHANGES REHABILITATION LLC.** managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **CHANGES REHABILITATION LLC.**'s Sanction Policy.

Remove Watermark Now
pdfelement