

HCA

DEPARTMENT: Information Technology & Services	POLICY DESCRIPTION: Information Confidentiality and Security Agreements
PAGE: 1 of 3	REPLACES POLICY DATED: 8/15/01, 11/1/01, 1/27/04, 4/30/05, 3/1/07, 12/1/07, 10/1/10
EFFECTIVE DATE: September 1, 2011	REFERENCE NUMBER: IS.SEC.005
APPROVED BY: Ethics and Compliance Policy Committee	

SCOPE: All Company-affiliated facilities including, but not limited to, hospitals, ambulatory surgery centers, physician practices, home health agencies, service centers, and all Corporate Departments, Groups and Divisions.

PURPOSE: To provide awareness of the importance of information security and confidentiality and to authorize and require agreements with individuals and external entities to protect Company systems and information resources, including confidential patient information.

POLICY:

- A. **Information Confidentiality and Security Agreements with Individuals.** The CSA forms acknowledge specific responsibilities the individual has in relation to information security and the protection of sensitive information, including confidential patient information, from unauthorized disclosure. These individual obligations support federal regulations for confidentiality and security, including the HIPAA Privacy and Security Rules.
1. All Company workforce members including employees, contractors, and volunteers who are granted access to Company information, or granted access to Company-provided systems must sign and abide by the employee Confidentiality and Security Agreement (CSA).
 2. All Company affiliated providers (not employed by Company) who are granted access to Company information, or granted access to the Internet through Company provided systems, must sign and abide by the Provider Confidentiality and Security Agreement (Provider CSA).
 3. A non-Company-employed provider, or other external entity may make and shall enforce such CSAs on behalf of employees working off-site (*e.g.*, contracted transcription service, electronic claims submissions support contractor, physician office practice), if stipulated in the Company's contract with the external entity (see B. below). Each individual working on Company premises and/or who is granted access to Company systems or Company Confidential or sensitive information (*e.g.*, patient information) must sign the Vendor CSA form.
 4. The CSA forms are official corporate documents and must not be altered in any manner without prior approval from Corporate Information Security.
- B. **Contracts with Business Partners.** Relationships with an external entity involving access to Company information and Company information systems or the exchange, transmission, or use of sensitive Company information require a formal contract including provisions to

HCA

DEPARTMENT: Information Technology & Services	POLICY DESCRIPTION: Information Confidentiality and Security Agreements
PAGE: 2 of 3	REPLACES POLICY DATED: 8/15/01, 11/1/01, 1/27/04, 4/30/05, 3/1/07, 12/1/07, 10/1/10
EFFECTIVE DATE: September 1, 2011	REFERENCE NUMBER: IS.SEC.005
APPROVED BY: Ethics and Compliance Policy Committee	

protect the confidentiality and security of the information and/or systems. For more information, refer to the Information Security - Vendor Information Security Agreement Policy, IS.SEC.008.

- C. **Contracts for IT&S Services.** All contracts for services will include appropriate standard security language approved by IT&S. Refer to Information Security - Vendor Information Security Agreement Policy, IS.SEC.008, and the Information Security Agreement (ISA) site on Atlas.
- D. **Sanctions.** Violations of this policy could lead to disciplinary measures up to and including termination of employment or business relationship. Suspected violations of this policy are to be handled in accordance with the Discipline section of the Code of Conduct. The Company encourages resolution at the local level and each Customer (an organization, business entity or organizational unit that has an established business relationship with IT&S as described in this policy's scope) will designate a process for reporting violations. In addition, violations may be reported to the Ethics Line at 1-800-455-1996.
- E. **Policy Exceptions.** Exceptions to Security Policy are to be submitted to Information Security for review and approval.

PROCEDURE:

- A. The CSA forms are posted and maintained by Information Security on the Company Intranet located under Security and are attached to this policy.
- B. Before an employee is granted any access to Company information or Company systems (except for access to an electronic CSA course), the employee must acknowledge the CSA. Acknowledgement consists of either signing a copy of the CSA form or, preferably, by completing the Confidentiality and Security Agreement online course (*e.g.*, Healthstream).
- C. Each physician and allied health professional must sign the Provider CSA at the time he or she is initially appointed to a facility's medical staff. Completed Provider CSAs will be maintained in the individual's credentials file, or signed and maintained electronically.
- D. Each volunteer must sign the CSA before beginning his or her service. The CSA signature process can be completed during Code of Conduct training (if the volunteer attends such training), volunteer orientation or separately. The completed CSA will be maintained with the Company's records of the volunteer's service, or signed and maintained electronically.
- E. Physician office staff must sign a CSA form at the time information access is granted. Completed CSAs must be maintained in a central location by the Physician Support Coordinator or individual with a similar role in the business unit.

HCA

DEPARTMENT: Information Technology & Services	POLICY DESCRIPTION: Information Confidentiality and Security Agreements
PAGE: 3 of 3	REPLACES POLICY DATED: 8/15/01, 11/1/01, 1/27/04, 4/30/05, 3/1/07, 12/1/07, 10/1/10
EFFECTIVE DATE: September 1, 2011	REFERENCE NUMBER: IS.SEC.005
APPROVED BY: Ethics and Compliance Policy Committee	

1. Providers must assign each member of their office staff a unique user ID to access Company systems, which is generated in accordance with Company procedures.
 2. Providers must notify Physician Support Coordinators within 24 hours or by the next business day about terminated office staff to ensure that their staff's user accounts to Company systems are appropriately disabled in accordance with Company standards and procedures for account termination.
- F. Representatives of vendors and other external entities must sign the Vendor CSA, or equivalent confidentiality agreement, when vendor representatives are assigned to work onsite with access to Company Confidential or Sensitive information, or if the individual vendor representative is granted access to Company systems (either onsite or remotely). The vendor representative must sign the Vendor CSA form (or equivalent) before information access or system access is granted. Completed Vendor CSAs must be maintained in the individual contract folder by the Facility CFO or designee, or signed and maintained electronically.
- G. All individuals listed in items B-E above may be required to re-sign the CSA when Corporate Information Security makes significant revisions to the CSA forms and those revisions are approved by the Ethics & Compliance Policy Committee.

REFERENCES:

1. [Code of Conduct Site](#)
2. Information Security – Program Requirements Policy, [IS.SEC.001](#)
3. [Information Security – Vendor Information Security Agreement \(ISA\) Policy, IS.SEC.008](#)
4. Information Security Standard – Vendor Contracts – COM.TPM.01
5. [Information Security ISA site on Atlas](#)
6. [Information Security Standards](#)
7. Information Security Standards – [Workforce Member Requirements Report](#)
8. Electronic Communications Policy, [IS.SEC.002](#)
9. Physician Access to the Internet Policy, [LL.026](#)
10. Copyright Policy, [LL.GEN.002](#)
11. Appropriate Use of Company Communications Resources and Systems Policy, [EC.026](#)
12. Non-Employee Dependent Healthcare Professionals Policy, CSG.QS.003
13. [“How to Encrypt Removable Media” Atlas site](#)
14. [“How to Encrypt Files” Atlas site](#)
15. [“How to Encrypt Emails” Atlas site](#)
16. [“Identifying Sensitive Data” Atlas site](#)
17. [InfoSec Issue Decision Form: Use of Non-Employee SSNs and DOBs](#)
18. [Mobile Device Guidance and Encryption Notification](#)

[Page Intentionally Left Blank]

Confidentiality and Security Agreement

Note: this form to be used for HCA employees and HCA workforce members.

I understand that the HCA affiliated facility or business entity (the "Company") for which I work, volunteer or provide services manages health information as part of its mission to treat patients. Further, I understand that the Company has a legal and ethical responsibility to safeguard the privacy of all patients and to protect the confidentiality of their patients' health information. Additionally, the Company must assure the confidentiality of its human resources, payroll, fiscal, research, internal reporting, strategic planning information, or any information that contains Social Security numbers, health insurance claim numbers, passwords, PINs, encryption keys, credit card or other financial account numbers (collectively, with patient identifiable health information, "Confidential Information").

In the course of my employment/assignment at the Company, I understand that I may come into the possession of this type of Confidential Information. I will access and use this information only when it is necessary to perform my job related duties in accordance with the Company's Privacy and Security Policies, which are available on the Company intranet (on the Security Page) and the Internet (under Ethics & Compliance). I further understand that I must sign and comply with this Agreement in order to obtain authorization for access to Confidential Information or Company systems.

General Rules

1. I will act in the best interest of the Company and in accordance with its Code of Conduct at all times during my relationship with the Company.
2. I understand that I should have no expectation of privacy when using Company information systems. The Company may log, access, review, and otherwise utilize information stored on or passing through its systems, including email, in order to manage systems and enforce security.
3. I understand that violation of this Agreement may result in disciplinary action, up to and including termination of employment, suspension, and loss of privileges, and/or termination of authorization to work within the Company, in accordance with the Company's policies.

Protecting Confidential Information

4. I will not disclose or discuss any Confidential Information with others, including friends or family, who do not have a need to know it. I will not take media or documents containing Confidential Information home with me unless specifically authorized to do so as part of my job.
5. I will not publish or disclose any Confidential Information to others using personal email, or to any Internet sites, or through Internet blogs or sites such as Facebook or Twitter. I will only use such communication methods when explicitly authorized to do so in support of Company business and within the permitted uses of Confidential Information as governed by regulations such as HIPAA.
6. I will not in any way divulge, copy, release, sell, loan, alter, or destroy any Confidential Information except as properly authorized. I will only reuse or destroy media in accordance with Company Information Security Standards and Company record retention policy.
7. In the course of treating patients, I may need to orally communicate health information to or about patients. While I understand that my first priority is treating patients, I will take reasonable safeguards to protect conversations from unauthorized listeners. Such safeguards include, but are not limited to: lowering my voice or using private rooms or areas where available.
8. I will not make any unauthorized transmissions, inquiries, modifications, or purgings of Confidential Information.
9. I will not transmit Confidential Information outside the Company network unless I am specifically authorized to do so as part of my job responsibilities. If I do transmit Confidential Information outside of the Company using email or other electronic communication methods, I will ensure that the Information is encrypted according to Company Information Security Standards.

Following Appropriate Access

10. I will only access or use systems or devices I am officially authorized to access, and will not demonstrate the operation or function of systems or devices to unauthorized individuals.
11. I will only access software systems to review patient records or Company information when I have a business need to know, as well as any necessary consent. By accessing a patient's record or Company information, I am affirmatively representing to the Company at the time of each access that I have the requisite business need to know and appropriate consent, and the Company may rely on that representation in granting such access to me.

Using Portable Devices and Removable Media

12. I will not copy or store Confidential Information on removable media or portable devices such as laptops, personal digital assistants (PDAs), cell phones, CDs, thumb drives, external hard drives, etc., unless specifically required to do so by my job. If I do copy or store Confidential Information on removable media, I will encrypt the information while it is on the media according to Company Information Security Standards

13. I understand that any mobile device (Smart phone, PDA, etc.) that synchronizes company data (e.g., Company email) may contain Confidential Information and as a result, must be protected. Because of this, I understand and agree that the Company has the right to:
 - a. Require the use of only encryption capable devices.
 - b. Prohibit data synchronization to devices that are not encryption capable or do not support the required security controls.
 - c. Implement encryption and apply other necessary security controls (such as an access PIN and automatic locking) on any mobile device that synchronizes company data regardless of it being a Company or personally owned device.
 - d. Remotely "wipe" any synchronized device that: has been lost, stolen or belongs to a terminated employee or affiliated partner.
 - e. Restrict access to any mobile application that poses a security risk to the Company network.

Doing My Part – Personal Security

14. I understand that I will be assigned a unique identifier (e.g., 3-4 User ID) to track my access and use of Confidential Information and that the identifier is associated with my personal data provided as part of the initial and/or periodic credentialing and/or employment verification processes.
15. I will:
 - a. Use only my officially assigned User-ID and password (and/or token (e.g., SecurID card)).
 - b. Use only approved licensed software.
 - c. Use a device with virus protection software.
16. I will never:
 - a. Disclose passwords, PINs, or access codes.
 - b. Use tools or techniques to break/exploit security measures.
 - c. Connect unauthorized systems or devices to the Company network.
17. I will practice good workstation security measures such as locking up diskettes when not in use, using screen savers with activated passwords, positioning screens away from public view.
18. I will immediately notify my manager, Facility Information Security Official (FISO), Director of Information Security Operations (DISO), or Facility or Corporate Client Support Services (CSS) help desk if:
 - a. my password has been seen, disclosed, or otherwise compromised;
 - b. media with Confidential Information stored on it has been lost or stolen;
 - c. I suspect a virus infection on any system;
 - d. I am aware of any activity that violates this agreement, privacy and security policies; or
 - e. I am aware of any other incident that could possibly have any adverse impact on Confidential Information or Company systems.

Upon Termination

19. I agree that my obligations under this Agreement will continue after termination of my employment, expiration of my contract, or my relationship ceases with the Company.
20. Upon termination, I will immediately return any documents or media containing Confidential Information to the Company.
21. I understand that I have no right to any ownership interest in any Confidential Information accessed or created by me during and in the scope of my relationship with the Company.

By signing this document, I acknowledge that I have read this Agreement and I agree to comply with all the terms and conditions stated above.

Employee/Workforce Member Signature	Facility Name and COID	Date
Employee/Workforce Member Printed Name	Business Entity Name	

Provider Confidentiality and Security Agreement

Note: this form to be used for non-employed physicians, providers and their non-HCA-employed staff.

I understand that the HCA affiliated facility or business entity (the "Company") at which I have privileges or for which I work, volunteer or provide services manages health information as part of its mission to treat patients. Further, I understand that the Company has a legal and ethical responsibility to safeguard the privacy of all patients and to protect the confidentiality of their patients' health information. Additionally, the Company must assure the confidentiality of its human resources, payroll, fiscal, research, internal reporting, strategic planning information, or any information that contains Social Security numbers, health insurance claim numbers, passwords, PINs, encryption keys, credit card or other financial account numbers (collectively, with patient identifiable health information, "Confidential Information").

In the course of my affiliation or employment with the Company, I understand that I may come into the possession of this type of Confidential Information. I will access and use this information only when it is necessary to perform my job related duties in accordance with the Company's Privacy and Security Policies, which are available on the Company intranet (on the Security Page) and the Internet (under Ethics & Compliance). I further understand that I must sign and comply with this Agreement in order to obtain authorization for access to Confidential Information or Company provided systems.

General Rules

1. I will act in accordance with the Company's Code of Conduct at all times during my relationship with the Company.
2. I understand that I should have no expectation of privacy when using Company information systems. The Company may log, access, review, and otherwise utilize information stored on or passing through its systems, including email, in order to manage systems and enforce security.
3. I understand that violation of this Agreement may result in disciplinary action, up to and including termination of employment, suspension, and loss of privileges, and/or termination of authorization to work within the Company, in accordance with the Company's policies.
4. I have no intention of varying the volume or value of referrals I make to the Company in exchange for Internet access service or for access to any other Company information.
5. I have not agreed, in writing or otherwise, to accept Internet access in exchange for the referral to the Company of any patients or other business.
6. I understand that the Company may decide at any time without notice to no longer provide access to any systems to physicians on the medical staff unless other contracts or agreements state otherwise. I understand that if I am no longer a member of the facility's medical staff, I may no longer use the facility's equipment to access the Internet.

Protecting Confidential Information

7. I will not disclose or discuss any Confidential Information with others, including friends or family, who do not have a need to know it. I will not take media or documents containing Confidential Information home with me unless specifically authorized to do so as part of my job.
8. I will not publish or disclose any Confidential Information to others using personal email, or to any Internet sites, or through Internet blogs or sites such as Facebook or Twitter. I will only use such communication methods when explicitly authorized to do so in support of Company business and within the permitted uses of Confidential Information as governed by regulations such as HIPAA.
9. I will not in any way divulge, copy, release, sell, loan, alter, or destroy any Confidential Information except as properly authorized. I will only reuse or destroy media in accordance with Company Information Security Standards.
10. In the course of treating patients, I may need to orally communicate health information to or about patients. While I understand that my first priority is treating patients, I will take reasonable safeguards to protect conversations from unauthorized listeners. Such safeguards include, but are not limited to: lowering my voice or using private rooms or areas where available.
11. I will not make any unauthorized transmissions, inquiries, modifications, or purgings of Confidential Information.
12. I will secure electronic communications by transmitting Confidential Information only to authorized entities, in accordance with industry-approved security standards, such as encryption.

Following Appropriate Access

13. I will only access or use systems or devices I am officially authorized to access, will only do so for the purpose of delivery of medical services at this facility, and will not demonstrate the operation or function of systems or devices to unauthorized individuals.
14. I will only access software systems to review patient records or Company information when I have a business need to know, as well as any necessary consent. By accessing a patient's record or Company information, I am affirmatively representing to the Company at the time of each access that I have the requisite business need to know and appropriate consent, and the Company may rely on that representation in granting such access to me.

15. I will insure that only appropriate personnel in my office, who have been through a screening process, will access the Company software systems and Confidential Information and I will annually train such personnel on issues related to patient confidentiality and access.
16. I will accept full responsibility for the actions of my employees who may access the Company software systems and Confidential Information.
17. I agree that if I, or my staff, stores Confidential Information on non-Company media or devices (e.g., PDAs, laptops) or transmits data outside of the Company network, that the data then becomes my sole responsibility to protect according to federal regulations, and I will take full accountability for any data loss or breach.

Doing My Part – Personal Security

18. I understand that I will be assigned a unique identifier (e.g., 3-4 User ID) to track my access and use of Confidential Information and that the identifier is associated with my personal data provided as part of the initial and/or periodic credentialing and/or employment verification processes.
19. I will ensure that members of my office staff use a unique identifier to access Confidential Information.
20. I will:
 - a. Use only my officially assigned User-ID and password (and/or token (e.g., SecurID card)).
 - b. Use only approved licensed software.
 - c. Use a device with virus protection software.
21. I will never:
 - a. Disclose passwords, PINs, or access codes.
 - b. Use tools or techniques to break/exploit security measures.
 - c. Connect unauthorized systems or devices to the Company network.
22. I will practice good workstation security measures such as locking up diskettes when not in use, using screen savers with activated passwords appropriately, and positioning screens away from public view.
23. I will immediately notify my manager, Facility Information Security Official (FISO), Director of Information Security Operations (DISO), or Facility or Corporate Client Support Services (CSS) help desk if:
 - a. my password has been seen, disclosed, or otherwise compromised
 - b. media with Confidential Information stored on it has been lost or stolen;
 - c. I suspect a virus infection on any system;
 - d. I am aware of any activity that violates this agreement, privacy and security policies; or
 - e. I am aware of any other incident that could possibly have any adverse impact on Confidential Information or Company systems.

Upon Termination

24. I agree to notify my Physician Support Coordinator within 24 hours, or the next business day, when members of my office staff are terminated, so that user accounts to Company systems are appropriately disabled in accordance with Company standards.
25. I agree that my obligations under this Agreement will continue after termination of my employment, expiration of my contract, or my relationship ceases with the Company.
26. Upon termination, I will immediately return any documents or media containing Confidential Information to the Company.
27. I understand that I have no right to any ownership interest in any Confidential Information accessed or created by me during and in the scope of my relationship with the Company.

By signing this document, I acknowledge that I have read this Agreement and I agree to comply with all the terms and conditions stated above.

Provider Signature		Date
Provider Printed Name		

Vendor Confidentiality and Security Agreement

Note: this form to be used for individual vendor representatives.

I understand that the HCA affiliated facility or business entity (the "Company") for which I provide services, manages health information as part of its mission to treat patients. Further, I understand that the Company has a legal and ethical responsibility to safeguard the privacy of all patients and to protect the confidentiality of their patients' health information. Additionally, the Company must assure the confidentiality of its human resources, payroll, fiscal, research, internal reporting, strategic planning information, or any information that contains Social Security numbers, health insurance claim numbers, passwords, PINs, encryption keys, credit card or other financial account numbers (collectively, with patient identifiable health information, "Confidential Information").

In the course of my assignment at the Company, I understand that I may come into the possession of this type of Confidential Information. I will access and use this information only when it is necessary to perform my job related duties in accordance with the Company's Privacy and Security Policies, which are available on the Company intranet (on the Security Page) and the Internet (under Ethics & Compliance). I further understand that I must sign and comply with this Agreement in order to obtain authorization for access to Confidential Information or Company systems.

General Rules

1. I will act in accordance with the Company's Code of Conduct at all times during my relationship with the Company.
2. I understand that I should have no expectation of privacy when using Company information systems. The Company may log, access, review, and otherwise utilize information stored on or passing through its systems, including email, in order to manage systems and enforce security.
3. I understand that violation of this Agreement may result in disciplinary action, up to and including termination of privileges, and/or termination of authorization to work within the Company facility or with Company data.

Protecting Confidential Information

4. I will not disclose or discuss any Confidential Information with others, including friends or family, who do not have a need to know it. I will not take media or documents containing Confidential Information home with me unless specifically authorized to do so as part of my job.
5. I will not publish or disclose any Confidential Information to others using personal email, or to any Internet sites, or through Internet blogs or sites such as Facebook or Twitter. I will only use such communication methods when explicitly authorized to do so in support of Company business and within the permitted uses of Confidential Information as governed by regulations such as HIPAA.
6. I will not in any way divulge, copy, release, sell, loan, alter, or destroy any Confidential Information except as properly authorized. I will only reuse or destroy media in accordance with Company Information Security Standards and Company record retention policy (provided upon request).
7. I will not make any unauthorized transmissions, inquiries, modifications, or purgings of Confidential Information.
8. I will not transmit Confidential Information outside the Company network unless I am specifically authorized to do so as part of my job responsibilities. If I do transmit Confidential Information outside of the Company using email or other electronic communication methods, I will ensure that the Information is encrypted according to Company Information Security Standards (provided upon request).

Following Appropriate Access

9. I will only access or use systems or devices I am officially authorized to access, and will not demonstrate the operation or function of systems or devices to unauthorized individuals.
10. I will not attempt to bypass Company security controls.
11. I will only access software systems to review Company information when I have a business need to know, as well as any necessary consent. By accessing Company information, I am affirmatively representing to the Company at the time of each access that I have the requisite business need to know and appropriate consent, and the Company may rely on that representation in granting such access to me.

Using Portable Devices and Removable Media

12. I will not copy or store Confidential Information on removable media or portable devices such as laptops, personal digital assistants (PDAs), cell phones, CDs, thumb drives, external hard drives, etc., unless specifically required to do so by my job assignment. If I do copy or store Confidential Information on removable media, I will encrypt the information while it is on the media according to Company Information Security Standards (provided upon request).

13. I understand that any mobile device (Smart phone, PDA, etc.) that synchronizes Company data (e.g., Company email) may contain Confidential Information and as a result, must be protected. Because of this, I understand and agree that the Company has the right to:
 - a. Require the use of only encryption capable devices.
 - b. Prohibit data synchronization to devices that are not encryption capable or do not support the required security controls.
 - c. Implement encryption and apply other necessary security controls (such as an access PIN and automatic locking) on any mobile device that synchronizes company data regardless of it being a Company or personally owned device.
 - d. Remotely "wipe" any synchronized device that: has been lost, stolen or belongs to a terminated employee or affiliated partner.
 - e. Restrict access to any mobile application that poses a security risk to the Company network.

Doing My Part – Personal Security

14. I understand that I will be assigned a unique identifier (e.g., 3-4 User ID) to track my access and use of Confidential Information and that the identifier is associated with my personal data.
15. I will:
 - a. Use only my officially assigned User-ID and password (and/or token (e.g., SecurID card)).
 - b. Use only approved licensed software.
 - c. Use a device with virus protection software.
16. I will never:
 - a. Disclose passwords, PINs, or access codes.
 - b. Use tools or techniques to break/exploit security measures.
 - c. Connect unauthorized systems or devices to the Company network.
17. I will practice good workstation security measures such as locking up diskettes when not in use, using screen savers with activated passwords, positioning screens away from public view.
18. I will immediately notify the Company facility’s Facility Information Security Official (FISO), Director of Information Security Operations (DISO), or Facility or Corporate Client Support Services (CSS) help desk if:
 - a. my password has been seen, disclosed, or otherwise compromised;
 - b. media with Confidential Information stored on it has been lost or stolen;
 - c. I suspect a virus infection on any system;
 - d. I am aware of any activity that violates this agreement, privacy and security policies; or
 - e. I am aware of any other incident that could possibly have any adverse impact on Confidential Information or Company systems.

Upon Termination

19. I agree that my obligations under this Agreement will continue after termination of my employment, expiration of my contract, or my relationship ceases with the Company.
20. Upon termination, I will immediately return any documents or media containing Confidential Information to the Company.
21. I understand that I have no right to any ownership interest in any Confidential Information accessed or created by me during and in the scope of my relationship with the Company.

By signing this document, I acknowledge that I have read this Agreement and I agree to comply with all the terms and conditions stated above.

Vendor Signature	Facility Name and COID	Date
Vendor Printed Name	Business Entity Name	