Credentials Verification Services Policies & Procedures Manual

OPERATIONAL AND FUNCTIONAL PROCEDURES

Claire Covelli
HOSPITAL SERVICES CORPORATION |

HSC

efficient^n

Introduction

Hospital Services Corporation (HSC) assists hospitals, managed care organizations and other provider groups with credentials verification for health care practitioners. This credentialing process consists of gathering and verifying specific information in accordance with the standards developed by the Joint Commission for Accreditation of Healthcare Organizations (the Joint Commission), the National Committee for Quality Assurance (NCQA), the Utilization Review Accreditation Commission (URAC), DNV Healthcare (DNV), and applicable state and federal regulatory requirements. HSC does not currently sub-delegate its credentialing activities.

HSC has a custom-designed software application known as eCreds that was developed to maintain the information necessary for the credentials verification process. The following procedures are designed to provide our employees with the standards and guidelines to be used in the credentials verification process on behalf of our customers.

These policies and procedures are reviewed on an on-going basis, but no less than annually, based upon a review of applicable standards and regulations[1]. As the policies and procedures are updated due to operational and/or regulatory requirements, they are distributed electronically to each staff person, and posted on our Intranet, HSCnet. All changes are discussed with the credentials verification services staff during the revision process, with subsequent changes discussed at applicable monthly staff meetings. Whenever revisions are made, the policies and procedures are formally approved by the President of HSC. Approval is not needed if no revisions are made to the current document during the review process. The President of HSC is authorized to approve the procedures by virtue of their position as the highest executive officer of the organization.

This document is subject to contractual obligations regarding confidentiality and shall not be forwarded outside HSC or a customer organization without the permission of the CVS Manager or the company President.

______________________________ [2] September 30, 2022
Erika Campos, President Date

Effective: June 1, 1996
Last Revised: September 2022
Reviewed: September 2021
Revised: September 2020

[1] CVO 1: Element A. 7.
[2] CVO 1: Element B.

Hospital Services Corporation
Policies and Procedures

Contents

I. Regulatory Compliance Requirements

The Joint Commission Introduction

Hospital customers are governed by the standards developed by the Joint Commission for Accreditation of Health Care Organizations (the Joint Commission) or Det Norske Veritas Healthcare (DNV). Some customers may also comply with the standards established by the National Committee for Quality Assurance (NCQA), the Utilization Review Accreditation Committee (URAC), or other standards.

Hospital customers that request credentials verifications are typically in the process of either recruiting new practitioners or ensuring that current practitioners are accurately and timely recredentialed. The contractual turn-around time for any file is sixty (60) days or less. All files, except for licensing board files, must comply with the applicable NCQA 120-day or 305-day rule and all other NCQA standards. Hospital customer files or other customer types of files may be reviewed by NCQA as substitution files during a survey in the same manner as managed care files and evaluated against all applicable NCQA standards to ensure that timely file follow-up is conducted. Our software system, eCreds, tracks the process of every file from beginning to end. A diary date interval is usually 10 to 25 working days, depending on the type of file and whether a file is to be expedited. Once a new application, including the release and attestation, has been entered into eCreds and then initiated, the verification requests will be generated by the system. Subsequently, eCreds will automatically generate follow-up letters for those verifications not received in specified intervals. Depending on the item needed, it may be necessary to contact the practitioner directly. All documents received in connection with the credentials verification process must be date stamped on the date they are received.

NCQA Introduction

Managed Care Organization (MCO) and Managed Behavioral Healthcare Organization (MBHO) customers are governed by the standards developed by the National Committee for Quality Assurance (NCQA). HSC contracts with these customers to obtain credentials information for practitioners applying for panel membership with these organizations.

The National Committee for Quality Assurance (NCQA) was developed to monitor and ensure these customers effectively maintain a mechanism to continually measure quality and improvement in the services they provide. Credentialing is one of the areas that NCQA monitors. MCOs must follow specific guidelines to be NCQA accredited. MBHOs must also follow specific guidelines to be NCQA accredited. Credentials Verification Organizations (CVOs) are given specific guidelines and standards to adhere to and may be NCQA certified. HSC incorporates NCQA guidelines in its credentials processes for both initial and recredentials files to ensure not only its own integrity, but the integrity of those who contract with HSC for credentials services. For answers to specific questions, contact NCQA.

NCQA Managed Behavioral Healthcare Organizations Introduction

The facilities and institutions addressed under these standards may be hospitals, residential treatment centers, residential rehabilitation centers, or other similar behavioral health organizations.

State Licensing Board Introduction

Licensing board customers follow standards established by applicable state statutes and regulations.

General Policies

Timelines[3]

All primary source verifications must be *performed* and/or *received* within 120 days from the date of the practitioner's attestation, which is attached to the application form or application update document. The applicant's work history, application, and attestation must be obtained within 305 days of the date of the

[3] CVO 1: Element A, 2 & 4.

application and attestation at the time the file is shipped so that these documents are not more than 365 days old at the time of the customer's credentials committee review. The applicant must attest to the correctness and completeness of the application content. Therefore, an attestation must always be included with the application. Except for the work history, application, and attestation, credentials primary source verifications may not be more than 120 days old at the time the file is shipped so that the information is not more than 180 days old at the time of the customer's credentials committee review. *Static credentials*, such as evidence of medical school graduation or completion of a residency, need to be verified only once and may be provided to numerous customers. These time-sensitivity standards are built into our software system requirements, and files will not move to the audit queue unless the required elements meet the applicable age requirements. For each file that reaches audit, a short profile is generated by the system which summarizes the credentials reviewed and that are included in the completed file. At the time the file is audited, it is the responsibility of the analyst auditing the file to review all file requirements for timeliness and accuracy. This is accomplished by reviewing the application against the file profile, and the profile against the file contents. Detailed audit policies and procedures have been compiled to assist with this process.

Electronic mailroom and diary system

All documents received by email, fax, mail, or uploaded in connection with the credentials verification process must be date stamped on the date they are received. All phone verifications must indicate the current date and name or initials of the verifying party. Verifications should be signed or initialed by the employee conducting the verification. Electronic signatures are acceptable. To ensure that a timely and proper amount of follow-up is conducted, a diary system is in place. Every file has an initiate date, diary intervals, and a completed date. This tracks the progress of the file from beginning to end. A diary date interval is usually 10 to 25 working days, depending on the type of file, the type of document, and whether a file is to be expedited. The credentials file work process for follow-up is based on the age of the file and the documents or verification items that are still needed to complete the file, and the stage that the file is in. This ensures that all files are continuously being monitored. Follow up may also be triggered by receipt of updated contact information from customers, providers or third parties, or by status and follow up requests direct from customers.

Queues

Files are monitored at various stages of the life cycle through use of different activity queues and follow-up tasks within eCreds. Customers can also see the status of the file and the items that have been received or are missing through the eCreds secure Customer Portal. This allows customers to assist with non-responding practitioners. Activity queues in eCreds include Mailroom, Input, Upload, Initiate, Follow-Up, and Audit. Within the Follow-Up queue, tasks are organized by type and source. Ownership of specific queues, resource allocation and workflow are handled through formal task allocation, weekly analyst huddles and daily review and assessment of operations by the operations coordinator and program manager.[4]

Types of Practitioners to be Credentialed[5]

The Joint Commission

The following practitioner types are to be credentialed within the scope of the Joint Commission requirements: physicians (MDs, DOs), dentists (DDSs), podiatrists (DPMs), chiropractors (DCs), psychiatrists or physicians certified in addiction medicine (MDs and DOs), licensed or certified psychologists (MAs, or PhDs), licensed or certified clinical social workers (MSWs), licensed clinical nurse specialists (MSNs), licensed psychiatric nurse practitioners (NPs), physical therapists (PTs), occupational therapists (OTs), and surgical technicians (STs) as well as other licensed, certified or registered behavioral healthcare specialists and any other professional as requested by the customer.

[4] CVO 1: Element A, 2 & 3
[5] CVO 1: Element A, 1.

NCQA MCO

The following practitioner types are to be credentialed within the scope of NCQA requirements: physicians (MDs, DOs), dentists (DDSs), podiatrists (DPMs), chiropractors (DCs), nurse practitioners (NPs), psychiatrists or physicians certified in addiction medicine (MDs and DOs), licensed or certified psychologists (PsychDs, MAs, or PhDs), licensed or certified clinical social workers (MSWs), licensed clinical nurse specialists (MSNs), licensed psychiatric nurse practitioners (NPs), physical therapists (PTs), other licensed, certified or registered behavioral healthcare specialists and any other professional as requested by the customer.

NCQA MBHO

The following practitioner types are to be credentialed within the scope of NCQA MBHO requirements: psychiatrists and other physicians, addiction medicine specialists, doctoral or master's level psychologists, master's level clinical social workers who are state certified or licensed, master's level clinical nurse specialists or psychiatric nurse practitioners who are state certified or licensed to practice independently, and other behavioral health specialists who are state certified or licensed to practice independently.

Licensing Customers

Both MDs and DOs are credentialed within the scope of State Licensing Board rules and regulations, as well as any applicable Federal guidelines.

Credentials to be Primary Source Verified [6]

HSC ensures that our credentials application captures information necessary to comply with credentialing standards. The information listed below includes elements required in applications we offer for use by our customers. Most of our customers use the HSC application. Others use State-mandated applications or customer specific application forms required by their facility bylaws and rules and regulations. The application from CAQH can also be utilized. Regardless of which application a customer uses, the attestation and release must match the application form that is being used. It is extremely important to note that the Joint Commission and NCQA require that the following credentials be verified from approved primary sources in full accordance with the standards set forth by the current published regulatory standards by the Joint Commission and NCQA:

- *Practitioner application with attestation and authorization to release information (obtained but not primary source verified)*
- *Licensure and medical board sanctions*
- *Hospital clinical privileges (obtained but not primary source verified)*
- *Primary specialty certification, board certification or residency completion/graduation from medical or professional school*
- *Professional liability claims history (through the NPDB)*
- *Evidence of current medical malpractice insurance coverage (copy of face sheet or declaration page or as indicated on the practitioner's application)*
- *DEA and/or state drug license certificates (CSR), or CSR verification, if applicable*
- *Work history (evident on a resume/CV/application for previous 5 years)*
- *Specialized training (MBHO only)*
- *National Practitioner Data Bank query (or Federation of State Medical Boards, if appropriate)*
- *Medicare and Medicaid sanctions (based on the NPDB query)*

[6] CVO 1: Element A, 1.

Note: NCQA does not require that the DEA certificate or the CSR certificate be primary source verified, and a copy of either certificate is valid. A current legible copy of either of these certificates or primary source verification of a CSR is sufficient.

Individuals Responsible for Conducting Verifications[7]

The Credentials Verification Services staff is responsible for processing credentials files, and the program manager is responsible for overseeing and ensuring all verifications are done in accordance with the applicable regulatory standards. All credentials department staff members understand and attest to their understanding of the necessity of adhering to our core principles which include maintaining confidentiality of the information, ensuring document integrity, and fulfilling the needs of our customers based on regulatory standards.

Methods Used to Access and Verify Credentials Information[8]

Staff members utilize methods described herein to access approved verification websites, contact appropriate sources, and process information in accordance with policy and procedures established with the intent of meeting all regulatory standards and customer expectations for quality, accuracy, and timeliness. All staff receive a thorough orientation and training specific to their core duties. As well as having workflows and queues managed within our credentialing system to ensure that the appropriate verifications are collected timely, we also have policies and procedures, tools and checklists that assist our team in completing activities consistently and appropriately. All information is maintained electronically within eCreds, and all data and documents included in the final credentialing file are thoroughly audited by a senior analyst to ensure that the appropriate standards are being met. Completed files are made available to our customers through the Customer Portal within eCreds.

Sources Used for Verifying Credentials[9]

Several web-based sources are utilized to verify credentials from the appropriate primary source. The URL's for these sources are included in eCreds, along with the login and password. For sources that change more frequently, spreadsheets and lists of sites saved as browser favorites, ensure that the appropriate primary sources are used consistently. Where there are multiple sources available to verify certain credential types, staff will always use the primary method to ensure consistency on our files. Use of a secondary method, for example, use of the AMA profile to verify credentials other than education may be used either at customer request, or at our discretion to ensure timeliness of file completion. Web-based sources may be used to verify credentials for:

- *Affiliations and Work History*
- *Board Certifications*
- *Controlled Substance Registrations*
- *Education Verifications*
- *EPLS and OIG Sanctions*
- *License Verifications*
- *National Practitioner Data Bank*

HSC maintains the contact information for its credentials verification sources in eCreds. On-line, telephone and written verification sources are updated, as necessary, and include the latest recognized sources for verifications. These sources are maintained in the various tables for easy access by the analysts.

[7] CVO 1: Element A, 3.
[8] CVO 1: Element A, 4.
[9] CVO 1: Element A. 5.

Process for Reporting Credentials Information to Customers[10]

Customers have on-line access to various reports and grids through our eCreds Customer Portal that show the real-time status of practitioner files. Such reports include total files in process, files in ship pending status, recredentials files due in the next 30 days, rush files in process, total completed files in last 30 days, and files over 30 days old. Customers can also access roster information, upload documents, review what has been received or is missing from a file, print pre-populated applications, and change the status of a file. Completed files are also posted to the Customer Portal for easy and secure access.

It is imperative that customers are aware of adverse actions taken against a practitioner. Such actions may include:

- *Loss of license*
- *State sanctions, restrictions, and/or limitations in scope of practice, as defined by the state licensing authority*
- *Loss or limitation of hospital privileges*
- *Loss or surrender of a DEA or CSR registration*
- *Loss of malpractice insurance*
- *Medicare or Medicaid sanctions*
- *Professional liability claims settlement*

This information would typically be obtained by HSC on behalf of a customer during the initial appointment, reappointment, or continuous file maintenance process, as stipulated in HSC's contractual agreements with the customer. If, for instance, HSC contracts with a customer to perform only initial appointments and reappointments, HSC will notify the customer of any actions or sanctions discovered during these processes, but HSC will not continue to gather such information at any other time.

If HSC contracts with a customer for initial appointments and continuous file maintenance, then HSC will notify said customer of any actions or sanctions discovered during the initial appointment process, and thereafter upon verification of any expiring documents as stipulated in the contractual agreement. If HSC contracts with a customer for sanctions monitoring, HSC will notify this customer of any actions or sanctions discovered each time the available sanctions information is accessed and received by HSC. HSC is not responsible for notifying the customer of actions or sanctions that occur at any other time.

The customer and/or practitioner have the right to request resolution of errors in, or omissions of, data collected by HSC during the credentials verification process. However, HSC is not responsible for errors or omissions in data provided to us by the sources of such data. Any such requests will be tracked using our ticketing system, AutoTask. Where such changes to data are required, documentation of the reason for the change will be saved to the provider's file in eCreds to provide an audit trail of the change.

Verbal, Written and Internet Data Sources[11]

HSC uses verbal, written, and web-based data to verify credentials information. When using web-based verifications, credentials analysts must use the website of the appropriate NCQA approved source for that element. Verbal and website verifications require a statement in the credentialing file that is dated and either signed or initialed by the credentials analyst who verified the information. Electronic signature of documents is acceptable. This may come in the form of a document footer for those verifications that are obtained on-line if the web browser supports this feature. For verifications that are obtained electronically through eCreds, there will be a date stamp and header or footer to validate the verification.

[10] CVO 1: Element A. 6.

[11] CVO 1: Element A. 5

This includes the web address of the site that the verification was obtained from. Written verifications may take the form of a letter, fax, or documented review of cumulative reports, such as a roster, released by the primary source of credentialing data. For web-based and other electronic verifications, the date generated by the source when the information is retrieved is the date used by NCQA for determining timeliness of the verification.

On-going Sanctions Monitoring[12]

HSC obtains practitioner sanctions information from primary sources for those customers requesting this additional service. At a pre-established schedule, the following sanction types may be obtained:

- *Medicare and Medicaid sanctions from the OIG on-line sanctions report, or other sources as requested by the customer.*
- *Excluded parties from the Excluded Parties List System (EPLS)*
- *Professional licensure sanctions from the applicable state licensing authority such as the Board of Medical Examiners, the Board of Osteopathic Medicine, the Board of Chiropractic Medicine, and others, as requested by the customer.*

Additional detail regarding this process can be found in Section V: On-going Sanctions Monitoring Process.

II. Application Procedures[13]

Initial and Reappointment Applications

The customer must indicate to HSC which application (i.e., Customer's Application, HSC application, or other application) is to be used during the credentials verification process. If HSC already has the customer's practitioner in its database, HSC's pre-populated application may be sent to the practitioner for review and updates, new signature pages, and attestation. Alternatively, the practitioner may be directed to HSC's secure on-line application, which is pre-populated real time during its completion. Additionally, the practitioner may be directed to the customer's approved application and release, or to a state-mandated application. Regardless of the application used, a request letter is sent requesting the practitioner to complete the application, electronically or hard copy, sign the release and attestation, and return or submit to HSC along with the required accompanying documents. NCQA and the Joint Commission require that the application include a statement by the practitioner regarding reasons for any inability to perform the essential functions of the position, with or without accommodations; lack of present illegal drug use; history of loss of license and felony convictions; history of loss or limitation of privileges or disciplinary activity; and current malpractice insurance coverage.[14] These questions are included on HSC's electronic and hard copy statewide applications in the Professional Practice Questionnaire (PPQ) section of the application; the current malpractice insurance coverage is requested as an accompanying document. All State mandated applications used for credentialing feature these questions as part of the application.

The practitioner must attest to the correctness and completeness of the PPQs and application.[15] The NCQA 305-day aging rule[16] is applicable for the processing of practitioner applications and is measured from the date of the practitioner's attestation on the application. Affirmative responses to the PPQ must be accompanied by an explanation of the circumstances of that event. If supplied by the customer, a copy of their by-laws and/or policies and procedures or rules and regulations is also made available on-line.

[12] CVO 1: Element A. 5.
[13] CVO 1: Element A. 1-5
[14] CVO 12: Element A. 1-5.
[15] CVO 12: Element A. 6.
[16] CVO 12: Element A

If HSC does not receive the completed or updated application after a request has been sent to the practitioner, follow-up application request letters are automatically sent out at twenty-five (25)-day intervals. Our Customer Portal allows customers to view how many requests have been sent, and where the requests are being sent. In addition, email notifications are sent to the customer at the time the third application request is sent, so that they are aware of unresponsive practitioners. The customer can update the practitioner's information and push out additional requests for an application to the new contact location, if applicable.

NOTE: To enhance the usefulness and clarity of this document, it should be assumed that the following information detailing processing of an initial credentials file shall also apply to the processing of a recredentials file unless an exception is noted at the end of each section.

Curriculum Vitae/Resume/Work History[17]

Practitioners are required to provide work history as part of the initial application process. This work history may be provided on the application, a resume or curriculum vitae (CV) or another addendum. NCQA and The Joint Commission do not require primary source verification of the work history, although some customers may include this as a requirement. For NCQA files there must be five (5) years of work history, practice location history or affiliation history evident in the file either on the application, the curriculum vitae or resume, including the beginning and ending month and year for each work history position. If the practitioner has practiced less than five years, then the time requirement begins with the date of initial licensure. This history must have been obtained within 305 days of the practitioner's attestation of the application. HSC is not required to verify work history from primary sources for NCQA files, but NCQA requires a review of any work history gap of six (6) months or more, either verbally or in writing. NCQA allows for telephone clarification of such gaps in work history of less than one (1) year. Such communication will be documented appropriately as a verbal verification. Any work history gap that is or exceeds one (1) year in length must be clarified in writing.

***Recredentials Applications**:* Work history gap identification and verification is not required for NCQA recredentials files.

Delineation of Privileges

Privilege forms may be a component of the appointment packet for a hospital, clinic, or other Joint Commission customer. Privilege forms are specific to each customer. HSC will direct practitioners to our Practitioner Portal where they may download the appropriate privileges. The practitioner must complete and return the privilege forms with the application for appointment. Privilege request forms are not required for NCQA customers.

Follow-Up Requests

Many times it is necessary to follow up with the practitioner after receiving the application to obtain additional information. A follow-up letter is automatically generated by eCreds to request the missing information. We refer to this document as the "copy request letter." The primary source verification (PSV) process can begin if the application included the release and attestation.

Authorization/Release

The HSC release and attestation is made available on-line to the practitioner at the time that the application is being requested.[18] This release must be signed and dated by the practitioner before the processing of the file may begin, as it authorizes HSC to obtain information regarding the practitioner. The release may be used on behalf of multiple customers for up to 305 days after the date it was

[17] CVO 8

[18] CVO 12: Element A

originally signed by the practitioner. Signature stamps are not acceptable unless the practitioner is physically impaired, and the disability is documented in the practitioner's file if the practitioner uses a signature stamp.[19] Electronic signatures are acceptable. All releases received must be date stamped on the date they are received. Verification of board certification, drug registrations, licensure, and other publicly available information may begin prior to receipt of the release.

All documentation obtained by HSC on behalf of its customers is considered confidential and is maintained in accordance with the confidentiality provisions of HCQIA, HIPAA, the New Mexico and other states' equivalent of the Review Organizational Immunity Act, and the New Mexico and other states' equivalent of the Medical Practice Act. Information obtained by HSC is preserved and maintained exclusively for the benefit of HSC's customers. The information will be released to a third party only with the written consent of the customer and the applicant, pursuant to the Release form. Except for those items that are available as public records, HSC may not verify information on behalf of any customer without first obtaining the written consent of the applicant.[20]

Provisional or Temporary Credentialing

NCQA does not recognize provisional credentialing, therefore, HSC does not offer this service to its customers. However, upon request by a customer, HSC will process ship pending files or itemized requests.

Joint Commission customers with by-laws that require recredentialing to immediately take place one (1) year following the initial credentialing often refer to this group of practitioners as "provisional". In those cases the practitioners are tracked in the eCreds database as recredentials, and customers can amend their reappointment dates according to reflect the one-year credentialing cycle.

Primary Source Verifications

Note: Information that is deemed public record may be verified prior to receiving a practitioner's dated, written authorization or release. Such items may include professional licensure, board certification, and drug registrations.

Licensure[21]

All current professional licenses must be primary source verified through the state licensing agency. Primary source verification information specific to the practitioner's discipline must be downloaded from the appropriate website or documented on a license verification form. Practitioners are requested to list all previously and currently held licenses in all states. Verification of all licenses held will be completed for an initial appointment for a Joint Commission customer. For an NCQA file, verification of the practitioner's license must only be performed for those states where the practitioner provides care for members of the customer managed care organization. All license verifications will include information regarding previous or current sanctions, restrictions on licensure and/or limitations on the scope of license. Verification of licensure may begin prior to receipt of the release and approved on-line sources are acceptable to complete this task. HSC's analysts are provided with links to all available websites. If sanctions reports are indicated, a request via telephone or fax must be made to the Board to obtain the report if the sanctions report is not available on-line. Verifications may be electronically initialed and dated.

Recredentials Applications: For Joint Commission recredentials files, all licenses that were current during the interim recredentials period or since the last appointment will be verified.

[19] CVO 12: Element A
[20] CVO 3: Element A. 2.
[21] CVO 4: Element A

Minimum Acceptable Verification:
Verification of current license number, license sanctions, and expiration date through the appropriate licensure board within 120-day time limit.

Controlled Substance Registration (CSR) [22]
A copy of the controlled substance certificate may be provided by the practitioner. This certificate may be verified on-line, by telephone, or through written correspondence to the State Board of Pharmacy. HSC's analysts are provided links to all available websites.

Although HSC may obtain a copy of and verify the state-controlled substance registration (CSR), NCQA only requires that a copy of the state CSR or the DEA certificate be obtained, not both, and neither is required to be primary source verified. Therefore, in the event one of the drug registrations has been obtained by HSC for an NCQA file, the file will not be delayed and will be forwarded with the minimum required verification. A verification of the CSR may substitute for a copy of either the CSR or DEA.

Minimum Acceptable Verification:
Joint Commission: Verification of current state-controlled substance registration number, status of registration (i.e., active and in good standing), and expiration date through the State Board of Pharmacy, and a copy of the DEA.

NCQA: Copy of CSR or DEA, or CSR primary source verification. There is no time limit for verification of the CSR; the CSR or DEA certificate must be effective at the time of reporting to the customer.

Drug Enforcement Administration Certificate (DEA)[23]
A current copy of the certificate is obtained from the practitioner. DEA certificates do not need to be primary source verified. Some practitioners, such as radiologists and pathologists, may not have a DEA certificate. The DEA certificate does not have to be obtained within the 120-day NCQA time frame, but it must be current at the time of reporting to the customer.

Although HSC obtains a copy of the DEA certificate and verifies the state-controlled substance registration (CSR), NCQA only requires that a copy of the state CSR or the DEA certificate be obtained, not both, and neither is required to be primary source verified. Therefore, in the event one of the drug registrations has been obtained by HSC for an NCQA file, the file will not be delayed, and will be forwarded with the minimum required verification.

Minimum Acceptable Verification:
Joint Commission: Verification of Drug Enforcement Administration registration by obtaining a copy of current certificate, and primary source verification of the CSR.

NCQA: Copy of CSR or DEA, or CSR primary source verification. There is no time limit for verification of the CSR; the CSR or DEA certificate must be effective at the time of reporting to the customer.

Insurance Coverage and Claims History[24]
HSC must obtain a copy of the current malpractice coverage certificate that shows the policy dates and amount of coverage. The copy may be obtained from the malpractice insurance carrier or the practitioner.

For NCQA files, HSC must also verify a practitioner's claims history for the previous five (5) years by either querying the NPDB, or by obtaining written verification from the malpractice insurance carrier.

[22] CVO 5: Element A
[23] CVO 5: Element A
[24] CVO 9: Element A

For Joint Commission files, HSC requests five (5) years of claims history by contacting the insurance carriers directly, although the NPDB query is sufficient for this verification.

To obtain verification from the malpractice insurance carrier, we fax, email, or mail the request letter generated by eCreds to the insurance company, along with a copy of the signed release, requesting verification of current insurance coverage, expiration date, and policy limits, and a copy of the last five (5) years of claims history. If a practitioner has a claims history, it is be noted in eCreds in the appropriate section so that a notation prints on the profile that accompanies the completed file.

Minimum Acceptable Verification:
Verification of current insurance coverage, expiration date and limits from the insurance carrier or by obtaining a current insurance certificate from the practitioner. Verification of five (5) years of claims history through the insurance carrier or NPDB within the 120-day time limit. (Note: The Joint Commission requires evaluation of evidence of unusual patterns or excessive numbers of professional liability actions resulting in a judgement but does not dictate where to obtain the claims history.)

Board Certification[25]
Medical Doctors (MDs), Doctors of Osteopathy (DOs), Doctors of Dental Surgery (DDSs), Doctors of Dental Medicine (DMDs), Doctors of Podiatric Medicine (DPMs), Certified Nurse Practitioners (CNPs), Physician Assistants (PAs), Certified Nurse Midwives (CNMs), and other types of practitioners may all be board certified through a recognized board. Board certification may last for a period prescribed by the board or may never expire as determined by the board and noted on the verification statement. Verification of board certification may begin prior to receipt of the release and is subject to the 120-day rule.

Credentials applications inquire as to whether the practitioner is board certified and if so, in what area. The practitioner may also include a copy of a board certificate to indicate certification. If a practitioner states that he or she is, in fact, board certified, HSC verifies this information through the appropriate source, which may include on-line sites such as ABMS or others, or by fax, mail or telephone.

If a practitioner is board certified by a recognized board and this certification has been verified, then NCQA does not require further verification of education and training, as board certification is considered the highest level. Board certification for MDs and DOs must be verified by one of the following means:

- confirmation from the ABMS, its member boards, or through an official ABMS agent
- confirmation from the appropriate specialty board
- entry in the American Medical Association (AMA) Physician Master File
- entry in the American Osteopathic Association (AOA) Physician Master File
- utilization of the prescribed method dictated by the specific board

Board certification for other health care professionals is verified from the appropriate specialty board. At least annually, we must obtain written confirmation from the non-ABMS or non-AOA board that it performs primary source verification of education and training for the board to be recognized. Board certification is only required for practitioners that are certified by a recognized board. Some boards post this information on their websites so that this confirmation is readily available.

For Joint Commission customers we may verify technical certifications for providers such as Surgical Technicians or Surgical Assistants. At customer request we may also verify certification with non-recognized boards. In these cases, the verifications will be obtained in addition to the verification of education and will not be used *in lieu* of verification of education.

[25] CVO 7: Element A

Minimum Acceptable Verification:
Verification of primary specialty board certification through the appropriate primary source subject to the 120-day time frame.

Sub-specialty Board Certification

Sub-specialty certifications are verified in the same manner as primary specialty certifications.

Minimum Acceptable Verification:
Verification of sub-specialty board certification through the appropriate primary source subject to the 120-day time frame.

Education/Training[26]

For Joint Commission files, all relevant professional education and training must be primary source verified. For NCQA files, education and training need not be verified if a practitioner is board certified by a recognized board, unless otherwise stated in the contractual agreement with the customer. Board certification may be used to verify education and training only if that specialty board primary source verifies education and/or training. If a practitioner is not board certified, verification of completion of the highest level of education achieved will meet this requirement. For those practitioners who have not completed a residency program, verification of graduation from the medical/professional school fully meets this requirement for NCQA. Therefore, HSC will first determine if the practitioner is board certified by a recognized board, and if not, will then proceed to verify residency or medical/professional school. The procedures for verification of medical school and residency are identified below:

Recredentials Applications: Education verification is not required for recredentials files, unless for Joint Commission files, the program of education or training was in process at the time of initial credentialing and was subsequently completed since the initial credentials file was completed.

Medical School Graduation

Verification of medical/professional school graduation is required by the Joint Commission. For NCQA files, primary source verification of medical/osteopathic (professional) school is only necessary if the practitioner is not board certified or is certified by a non-physician specialty board and has not completed a residency. The application requests information regarding where the practitioner received his medical/professional degree. NCQA and the Joint Commission accept the AMA profile (MDs) and the AOA profile (DOs) as primary source verification of this information. The eCreds database will generate a letter to verify education if the verification is not available through an online source. Verification of medical/professional school graduation is considered a *static* verification. This means that medical/professional school graduation must only be verified once, and the information may be used for multiple customers since the verification does not expire. Verification of a fellowship or internship does not meet the intent of this element. Note that it is also possible to verify education and training from a state licensing agency if it performs primary source verification, and HSC can confirm primary source verification occurs directly from the agency.

Verify medical/osteopathic/professional education through the following sources:

- confirmation directly from the medical/osteopathic/professional school, or through an approved online source, for example, National Student Clearinghouse, that houses information on behalf of the school
- entry in the AMA Physician Master File
- entry in the AOA Physician Master File

[26] CVO 6: Element A

- confirmation from the state licensing agency if HSC ascertains that the state agency conducts primary source verification of education; or
- confirmation from the Educational Commission for Foreign Medical Graduates (ECFMG) for international medical graduates licensed after 1986

Exception: If a physician indicates that education and training was completed through the AMA's Fifth Pathway program, the education and training must be verified through the AMA. It is not acceptable to verify this type of education and training directly with the school.

Minimum Acceptable Verification:
Verification of medical/professional school graduation through written correspondence with the medical/professional school, telephone confirmation with the medical/professional school, or by obtaining a profile from the AMA or the AOA, or by obtaining verification from the ECFMG, as appropriate.

Residency

The application requests information regarding where the practitioner completed his internship and/or residency, which is referred to as post-graduate training. The Joint Commission also accepts the AMA profile or the AOA profile as primary source verification of this information. Verification of post-graduate training is considered a *static* verification. This means that this must only be verified once, and the information may be used for multiple customers since the verification does not expire. The Joint Commission requires that both the internship and residency be verified. For NCQA files, only the residency is required to be verified and that is if the practitioner is not board certified by a recognized board.

Verify completion of an internship (for Joint Commission files)/residency through the following sources:

Physicians/Osteopathic Physicians:

- confirmation from the internship/residency training program
- entry in the AMA Physician Master File
- entry in the AOA Physician Master File, or
- confirmation from the state licensing agency if HSC ascertains that the state agency conducts primary source verification of post-graduate training.

Minimum Acceptable Verification:
Verification of residency through written correspondence or telephone confirmation with the educational facility, or by obtaining a profile from the AMA or the AOA, or other state licensing agency, as applicable. For Joint Commission files, verification of an internship is also required utilizing these same sources.

Fellowship

The application requests information regarding where the practitioner completed his fellowship. Not all practitioners complete a fellowship. Where verification of a fellowship is required, HSC will send a letter generated by eCreds to verify that this information is accurate. The Joint Commission accepts the AMA profile and the AOA profile as primary source verification of this information. Verification of fellowship is considered a *static* verification. This means that the fellowship must only be verified once, and the information may be used for multiple customers since the verification does not expire. Verification of the fellowship is not required by NCQA and does not substitute as verification of the highest level of training but may be a customer requirement. If a practitioner completed both a residency and fellowship, HSC will only verify the residency unless we have a customer request to also verify the fellowship. In no case will a fellowship verification substitute for verification of the residency.

Minimum Acceptable Verification:
For Joint Commission files, verification of fellowship through written correspondence or telephone confirmation with the educational facility, or by obtaining a profile from the AMA.

Foreign Medical School Graduate

From time-to-time, a physician will have graduated from a foreign medical school that requires verification through the ECFMG. The practitioner will have been assigned an ECFMG number, which is needed for the verification letter. If the ECFMG number is not included on the application, it must be obtained from the physician. HSC will request ECFMG Certification on-line directly to ECFMG to verify medical school graduation. There is a charge for this verification. NCQA and the Joint Commission accept the AMA profile and the AOA profile as primary source verification of this information, and the ECFMG number is not necessary for this query. Canadian and Puerto Rican medical school graduates are not issued an ECFMG number; therefore, verification is performed directly with the Canadian or Puerto Rican medical school or facility. It typically takes from two (2) to three (3) weeks for this verification. Verification from the ECFMG is valid for only those practitioners licensed after 1986.

Minimum Acceptable Verification:
Verification of foreign medical school graduation through verification by the ECFMG.

Other Practitioners

Verification of professional school graduation is required by the Joint Commission. For NCQA files, primary source verification of professional school is only necessary if the practitioner is not board certified by a recognized board. The application requests information regarding where the practitioner received his professional degree. The eCreds software will generate a letter to verify that this information is accurate, unless the information is available from an approved online source, for example, National Student Clearinghouse. Verification of professional school graduation is considered a *static* verification. This means that professional school graduation must only be verified once, and the information may be used for multiple customers since the verification does not expire. Because the ECFMG does not include non-physician practitioners, foreign education may be obtained by contacting the foreign professional school or through the appropriate licensing board after confirmation that the licensing board primary source verified the education.

Verify professional education through the following sources:

- confirmation from the professional school
- confirmation from the appropriate licensing board after confirming that the licensing board primary source verified the education

Minimum Acceptable Verification:
Verification of professional school graduation through written or telephone confirmation with the professional school, online using a source approved by the school to handle verifications on their behalf, or through the appropriate licensing board after confirmation that the licensing board primary source verified the education.

Data Bank Queries (NPDB)[27]

The National Practitioner Data Bank (NPDB) is queried at the time of initial appointment, reappointment, and temporary privileges by specific customer request, or when the physician is requesting additional privileges. The Data Bank is used to query for any disciplinary actions taken, restrictions on licensure and limitations on scope of practice or claims against the practitioner, medical malpractice claims and

[27] CVOs 9, 10 and 11: Element A

settlement history, and whether there are any Medicaid/Medicare sanctions against the practitioner. Any actions taken against a practitioner before 1990 have not been reported to the Data Bank. The Data Bank query must be specific to each customer. In other words, *it is not acceptable to use one customer's query for another customer, or to use a self-query provided by the practitioner.* HSC obtains authorization to query on behalf of our customers.

All hospitals, health maintenance organizations and certain other approved organizations are authorized to query the NPDB. In some cases, however, a customer may not fall into the category of those organizations authorized to query the data bank. In these situations, the Federation of State Medical Boards (FSMB) may be queried, if specified by the customer.

Minimum Acceptable Verification:
Verification of actions/sanctions/malpractice claims history against a practitioner by querying the National Practitioner Data Bank within the 120-day time frame.

State Board Queries[28]
Physicians:
Regarding any previous or current state sanctions, restrictions on licensure, and/or limitations on scope of practice, HSC queries the following sources for sanctions or limitations on licensure:

- National Practitioner Data Bank (NPDB)
- Federation of State Medical Boards (FSMB)
- Or the appropriate state board or agency

Information on sanctions, restrictions on licensure, and/or limitations scope of practice must cover the most recent five (5)-year period available through the data source. If practitioners were licensed in more than one state in the most recent five (5)-year period, the query must include all states in which they worked. The query may be written or verbal. Verbal verification requires that the information received is documented on the applicable form, such as the *license verification form*, and that it be initialed by the credentials analyst. HSC will notify its customers of actions taken against a practitioner by including information on the profile that accompanies the completed credentials file when it is posted to the Customer Portal upon completion of a file.

Chiropractors:
Verification should come directly from one of the following sources:

- Appropriate State Board of Chiropractic Examiners
- National Practitioner Data Bank (NPDB)
- Or from the Federation of Chiropractic Licensing Boards' Chiropractic Information Network/Board Action Databank (CIN-BAD).

Oral Surgeons:
Verification should come directly from one of the following sources:

- Appropriate State Board of Dental Examiners or State Medical Board
- National Practitioner Data Bank (NPDB)

Podiatrists:
Verification should come directly from one of the following sources:

- Appropriate State Board of Podiatric Examiners
- National Practitioner Data Bank (NPDB)

[28] CVO 10: Element A

- Or the Federation of Podiatric Medical Boards

Other Non-physician Health Care Professionals:
Verification should come directly from one of the following sources:

- Appropriate state agency
- National Practitioner Data Bank (NPDB)
- State licensure or certification board

Note: Practitioner self-query does not satisfy this standard.

NCQA accepts the use of the Proactive Disclosure Service (PDS) of the National Practitioner Data Bank (NPDB) for verification of malpractice history, initial sanctions information, on-going monitoring, recredentialing verification of malpractice history, and limitations on licensure and sanction information.

Minimum Acceptable Verification:
Verification of licensure sanctions, restrictions and/or limitations on scope of practice for the previous five (5) years through the appropriate state licensing board, the appropriate databank, or approved state licensing or certification board.

Medicare/Medicaid Sanctions (NCQA)[29]
Verification of the practitioner's Medicare and Medicaid status is performed by conducting a NPDB query. At the request of a customer, HSC may verify Medicare/Medicaid status by accessing other sources, including:

- State Medicaid agency
- Medicare intermediary
- List of Excluded Individuals and Entities (OIG)
- Medicare Exclusion Database
- FSMB

Minimum Acceptable Verification:
Verification of Medicare/Medicaid sanctions through the NPDB within the 120-day time frame

Federation of State Medical Boards (FSMB)
Upon request, the Federation of State Medical Boards may be queried on behalf of a hospital or other customer for physicians and osteopathic physicians. This query assists our customers by providing additional information that might be useful during the credentialing process, including Medicare/Medicaid sanctions.

The FSMB may not specify the nature of the disciplinary action taken against a license. Specific information may be obtained from the appropriate medical board.

Minimum Acceptable Verification:
Verification of actions/sanctions against a practitioner by querying the FSMB within the 120-day time frame per customer request. Verification is only performed if required by the customer's contract.

Professional References

[29] CVO 11: Element A

The application for appointment will include the names and contact information of the practitioner's peer references. A letter is generated and sent by mail, fax, or email by the eCreds software to all references listed on the application with a copy of the practitioner's release.

Most customer specifications require two (2) references, but this can vary by customer. Practitioners must list references that are at least of the same professional discipline. For example, an MD must list three (3) to five (5) other MDs as references. NCQA does not require that professional references be obtained and an application that does not include listed references will not be delayed. However, some NCQA customers require that we request references on behalf of their practitioners.

Minimum Acceptable Verification:
Joint Commission: Written verification of professional references from the same professional discipline, as required by the customer standards.

NCQA: None

Hospital Affiliations (Joint Commission)
Unless available online, a letter is generated by eCreds to verify all current and previous hospital and institutional affiliations that the practitioner lists on his initial application, resume or curriculum vitae for the previous five (5) year period, or as specified in the contractual agreement with the customer. This requirement is not applicable for NCQA files.

Minimum Acceptable Verification
Joint Commission: Written, telephone, or on-line verification of all current and previous hospital and institutional affiliations for the period specified by the customer's requirements.

Primary Admitting Facility (NCQA)
Verbal or written confirmation from the practitioner's *primary* admitting facility that the practitioner has clinical privileges in good standing is not required by NCQA but may be required by NCQA customers. Verification includes the date of appointment, status of appointment and current standing. A letter is generated by eCreds for this verification. Written correspondence should be directed to the appropriate department of the facility.

The following types of practitioners may not have primary admitting facility privileges:

- Consulting physicians
- Locum tenens physicians
- Courtesy physicians
- Clinic physicians
- Dermatologists, radiologists, and pathologists (but not limited to these)
- Dentists
- Other licensed allied health professionals such as social workers, chiropractors, physical therapists, and counselors

Minimum Acceptable Verification:
If required by the NCQA customer, verification of clinical privileges in good standing from the practitioner's primary admitting facility by written correspondence, telephone, or roster verification within the 305-day time frame. A letter of explanation regarding admitting arrangements and signed by the admitting physician may also be acceptable.

File Completed and Audited[30]

Once all required information has been gathered for a practitioner and verified in line with customer requirements and applicable regulatory standards, each file is audited for completeness and accuracy. A file cannot be posted to the Customer Portal for download until it has successfully passed the audit process. Each completed file consists of a profile which summarizes the content of the file, as well as the application, supporting documents and credentials that have been collected and verified during the credentialing process.

The file audit steps are as follows:

- Review the electronic file against the profile and application, and perform a closing audit for accuracy, appropriateness, and completeness. If the file is determined to be compliant, the analyst will submit the file as "audit passed" and the electronic file will be posted to the secure Customer Portal for download
- If a credentials file is found to be non-compliant, the file will be flagged as "audit failed," which will return the file to normal flow for follow-up on the non-compliant items
- Once the file is corrected, it will be returned to the audit queue for final review again
- The file auditor then reviews file for corrections and submits the file as "audit passed," as appropriate

Once a file is completed the system emails the customer indicating that the file is complete and has been posted to the Customer Portal to be downloaded.

If the customer has asked for a file to be expedited and HSC is awaiting verifications, the customer may request that the file be set to "Ship Pending." The file will be audited and shipped to the customer, and any outstanding verifications will then be posted to the customer portal as soon as they are received. Customers may also request that a file be set to "Ship As-Is." The file will be audited and shipped to the customer, as is.

Roster Management

Customers can create and maintain their roster of active practitioners through the eCreds secure Customer Portal. To ensure that the correct practitioners are credentialed in a timely manner, it is the responsibility of the customer to update their roster with any changes that may impact the credentialing process. Mailing addresses, phone numbers and fax numbers, as well as next recredentialing dates need to be updated regularly to ensure that the roster is up to date. Practitioners may also need to be added to the roster or inactivated (termed) from the roster over time. Online reports and automated e-mails from our system inform customers of potentially unresponsive practitioners and assist customers in identifying roster information that may need to be updated. If the customer fails to notify HSC in a timely manner of changes to their roster, the customer may be billed for any credentialing activity (including file maintenance), that was completed prior to the notification of the change

III. Hospital Customer Temporary Privileges Verifications

Temporary privileges are issued by many Joint Commission customers to provide coverage for active staff or during other extenuating circumstances. If a customer indicates they need to privilege a practitioner temporarily, the customer will outline the process to be followed. Such requests are typically handled through our Itemized Request service. This service allows customers to request the verification of a subset of credentials rather than a full credentialing file. Appropriate items will be acquired and sent to the customer. HSC must have a valid, signed release from the practitioner to request, process and forward any required documents. We will continue to request, receive, and process remaining items to

[30] CVO 1: Element A. 6

complete the file in accordance with the Joint Commission or customer standards. These items are sent to the customer via mail, email, scanning and posting, or fax as they are received.

IV. File Maintenance Process

File Maintenance (FM) is a process offered to customers to obtain evidence of continued coverage in medical malpractice insurance and state and/or Federal drug registration programs, as well as verification of licensure in their practicing state and continued board certification, if applicable. eCreds tracks all expiration dates throughout the calendar year, generating verification letters or tasks for items that are expiring and must be re-verified. Verifications and evidence of continued certification are forwarded to the customer as they are received. This ensures that all licenses, board certifications, drug registrations, and malpractice insurance policies are kept current in the customer's files.

Copies and Primary Source Verifications

Practitioners are required to provide a copy of their renewed certificate of insurance (COI) when it expires. If a current copy of the DEA certificate is not available online, a copy must also be requested from the practitioner. A copy request letter will be sent by eCreds to the practitioner.

All verifications are subject to the same standards outlined previously. License verifications will include obtaining information regarding previous or current sanctions, restrictions, or limitations on the scope of practice.

Minimum Acceptable Verification:
File Maintenance items are subject to the same standards for minimum acceptable verification as outlined in previous sections for these elements.

Shipment of Documents

Items that have been verified upon expiration are posted to the Customer Portal for retrieval. The current copies and verifications are also available to always view on the Practitioner's page.

Non-Responding Practitioners

Due to the potential issue of practitioners not responding to requests for information in a timely manner, eCreds tracks the expirable items to more effectively monitor those practitioners whose files are not up to date regarding expirable items. Prior to the expiration of each file maintenance item, analysts responsible for file maintenance will contact the customer to inform them of any issues. We also continue to reach out to the practitioner to ensure that items are renewed. Customers can also see details of any expired or soon-to-expire items using reports available from the eCreds Customer Portal.

V. On-Going Sanctions Monitoring Process

Medicare, Medicaid, OIG, and Other Sanctions

HSC accesses the data directly from the primary sources, and then creates reports based on the collected information. Primary source data is imported into HSC's software system when it becomes publicly available. Current practitioners are checked against the sourced data, and when a practitioner is determined to be a possible match, the information is reviewed, and the findings are communicated to the customer. Customers can select the frequency of these reports depending on their needs.

Licensure Sanctions/Limitations

HSC queries the applicable state licensing boards for adverse findings at a frequency determined by the customer based on their needs. A summary report is created for the customer on completion of the monitoring activity. Sanctions are scanned within the file and kept in electronic format for future reference.

Customer Notification

If a customer's practitioner is listed on a report or other information source, or if the source information is determined to be inadequate or of poor quality, HSC will notify the customer. In-process files include sanctions alerts on the profile. Alerts and notifications include loss or limitation of license, sanctions (state, Medicare, Medicaid), and liability claims settlements.

Administration

The reporting of sanctions findings including loss or limitation of license, state sanctions, restrictions and/or limitations in scope of practice, as defined by each licensing agent and Medicare or Medicaid sanctions, will be sent to the customer upon receipt.

Copies of sanctions reports are maintained within the practitioner's records in eCreds. Information may be gained from: a) the normal processing of a file; b) an OIG/EPLS query which is done for customers that request this report for each file; c) a monthly query; or d) semi-annual sanctions monitoring.

VI. Staff Training [31]

HSC uses flex charts, training plans and training checklists to ensure that all staff receive the necessary training to carry out credentialing activities. The flex chart and training checklist also helps to ensure department and organizational sustainability in the event of turnover or expansion.

HSC has an intensive training program for its credentials analysts. The main activities cover orientation, follow-up, input, initiating, upload, auditing, and customer service training for analysts. Comprehensive procedures are used for training in the main file processing queues. Each member of the team is assigned core activities to ensure that all credentialing activities are covered so that customer needs are met.

Cross training provides flexibility to meet customer needs. Our Credentials Verification Program may use other HSC personnel for selected tasks to cover unexpected absenteeism or to meet short-term customer demands. Any new job duties must be added to the flex chart and training must occur. Flex charts are reviewed semi-annually during the annual and interim performance evaluation periods, or before the start of a new employee. This ensures that any added job duties are included in the flex chart.

Training plans tailored to the job duties of each position in the team are used to ensure all new employees are properly trained on all job functions within their position. The program manager has a combined department flex chart that lists each employee within the department, and his or her assigned activities.

HSC is committed to identifying and providing pertinent continuing education for our managers and staff. This may include the following, as well as other opportunities:

- Attendance and membership in the New Mexico Association of Medical Staff Services
- Attendance and participation in seminars and workshops
- Networking with local medical staff appointment personnel
- On-going certification education
- Attendance at customer User's Group Meetings

[31] CVO 1: Element A. 3.

VII. Continuous Quality Improvement[32]

HSC is a dynamic organization that enjoys an extremely close relationship with the health care community in multiple states.

Several elements form the backbone of our organizational approach to quality and apply to the entire organization, including the credentials verifications services program:

- Our Leadership Model
- Our Five Customer Commitments
- Our Strategic Planning Process
- Our Performance Management System

Strengths of the organization which contribute to the efficiency and quality of our programs include:

- Readily available access to management
- Quick response to customer requests and changes
- Close relationship and access to customers
- Back-up resources available throughout the organization

Every program manager meets with the President at least monthly to review progress and on-going issues involving the program including, but not limited to, marketing, customer satisfaction, financial progress, interpretation of standards, workload, productivity, quality, clerical support, and operations.

Each department within HSC structures, monitors, and organizes their quality initiatives using a standard approach:

- Reporting of operational performance monthly through the Management Dashboard, including action planning to address performance below target as well as barriers to improvement
- Management team meetings twice a month, scheduled to coincide with the project management meetings
- Tracking of key performance measures tied to company goals and objectives on the Monthly Scorecard and correlating Management Dashboard
- Handling of day-to-day customer interactions via customer service teams
- Recording of customer interactions and tracking of customer complaints or issues via our ticketing system, AutoTask
- Outreach to key customers as part of our customer management system
- Annual Customer Satisfaction Survey and ongoing mini surveys to obtain feedback on performance
- Individual meetings, customer visits, point of service communications and user group meetings to obtain feedback on customer needs and feedback on performance

Daily Core Activities

In addition to following the overall organizational approach to continuous internal quality improvement listed above, Credentials Verification Services has developed a model based around core daily activities and assignments for the team. Together, these activities enhance efficiency, quality of service and accuracy of reports to our customers.

Each member of the team is assigned daily core activities that tie ultimately to the company goals, the department's scorecard metrics, and individually assigned goals that form part of the performance management system at HSC.

Department Metrics

[32] CVO 2: Element A. 1,2 and 3.

In addition to department goals for budget and revenues, each year the key indicators we use internally to assess our performance are reviewed to ensure that they remain relevant to customer needs, department goals and company strategic direction. Target levels are reviewed to ensure that the measures are challenging and promote continuous improvement. For credentialing, key measures relate to file turnaround times, file quality as measured by daily file audits (that cover 100% of the file population), number of files shipped, efficient management of key file processing activities, as well as customer service activity. These indicators are used to monitor the progress and success of our program and to identify areas where there are opportunities for improvement.

Team Communication

Communication is a key part of the quality improvement focus. At the beginning of each month, the program manager emails the team covering key processes, performance indicators, barriers identified, and the goals for the month.

Weekly and monthly team meetings and huddles are conducted to keep all staff members informed. Subjects covered include:

- Changing regulatory standards
- Customer issues
- Software updates
- Review of monthly departmental and individual performance
- Audit fail reasons
- Training on areas identified for improvement
- Best practice recommendations and feedback.

In addition, all-staff meetings are held on a quarterly basis.

Team members are encouraged to brainstorm solutions to issues and areas identified for improvement. Our daily processes and procedures are reviewed dynamically so we can adjust and pivot to address the immediate needs of the customer. We do not have to wait for formal meetings to discuss issues; impromptu discussions help us to remain flexible in a fast-paced working environment.

Performance Evaluation and Management

The eCreds system tracks the queue status and work in process numbers real-time. These indicators are monitored daily to ensure that resources can be assigned appropriately, based on volume, so that customer needs are met. Productivity reports show areas where attention may be needed and is one of the ways individual quality and performance is monitored on an ongoing basis.

Each month the program manager meets with each employee to review and evaluate performance in relation to individual, team, and company goals. In addition to this continuous monitoring, performance is evaluated formally twice a year.

Evaluation of Customer Needs and Level of Satisfaction

Feedback regarding the quality and timeliness of HSC’s work is obtained in a variety of ways from customers. This on-going and frequent exchange of information takes place through telephone conversations and face-to-face meetings. HSC determines its customer requirements and expectations through direct interactions with customers and potential customers. These include the following activities:

- In-person visits
- Customer satisfaction surveys
- Customer user group meetings

- Board meetings
- Regularly scheduled communications that are part of our customer relationship management process

A key point of contact and communication with customers is our dedicated customer service team, which is described in more detail in a later section of this document.

Information gathered during these interactions and communications is used to validate current processes and to gather ideas for improvement and potential new services. Feedback can result in modifications to processes, updates and improvements to policies and procedures, and additional training on specific areas. Occasionally, improvements may take the form of additions to or changes to software that is used as part of the credentialing process. New features and automation of manual process are some of the ways we have been able to enhance quality and better meet customer needs. Customer training and development of better resources for customers is another way we look to enhance the experience for customers and partner more closely with them.

Customers are asked to participate in our customer satisfaction surveys across all business lines. Results of those surveys are collated, and comments shared with staff, management, and customers. Action plans are developed by each department, as needed, to address issues or concerns highlighted through customer feedback. We are adding point-of-service surveys to obtain immediate and ongoing feedback relevant to our daily operations.

Quality Assessment, Monitoring, and Identification of Opportunities for Improvement

Accuracy, timeliness, and quality of the credentials files which we complete for our customers are key items that we assess and monitor. These are the core of our department goals and our daily core activities. They are also the focus of our key performance indicators as tracked on our scorecard and reported out in various forums.

Our file audit process is the main method for ensuring that all files meet the applicable regulatory and customer requirements. Every file is subject to a full audit by a senior analyst prior to being sent to the customer. Files that do not meet the required standard are "audit failed" and returned to the file population. We log the reasons why a file fails the audit process in real-time. This daily audit of all files helps to identify issues with the quality and accuracy of data, verifications and documents that comprise the file. Through this process, systemic issues can quickly be identified. It is the role of the auditor to identify any apparent trends in the files which initially fail the audit process and communicate these to the program manager. This real-time review and analysis of files is the key to addressing any issues promptly.

By logging the reason for audit fails, we can track and trend quality issues over a longer period and determine the root causes and take steps to improve. The percentage of audit fails is tracked monthly and each quarter the results are reviewed and analyzed to identify opportunities for improvement. These findings may result in changes to processes and procedures or additional training, and the findings are reviewed with the team. This builds on the day-to-day adjustments we can make to operations because of auditor feedback.

We also perform monthly sample audits as an additional step to assess quality of the completed files. This helps us to ensure that our auditors are meeting the appropriate level of quality and skill needed to auditor files effectively.

On a quarterly basis we review and analyze audit fail/monthly sample audit failures to identify opportunities for improvement including the appropriate next steps to take to improve in specific areas.

These quarterly reviews are discussed during team meetings and huddles where the whole team can suggest new approaches and ways to address issues, as well as discussing barriers to improvement. Special audits or evaluation of data may be initiated as the result customer feedback, data analysis, and regulatory change, or based on observation of potential non-compliant circumstances identified by a variety of external and internal sources.

Another way to identify opportunities for improvement is through an assessment of feedback from the annual customer satisfaction survey. This assessment results in the development of action plans, where appropriate, if feedback is actionable. Our issue handling process may also provide valuable feedback on quality that can be reviewed and analyzed in a similar way, and then integrated back into our daily core activities through training, development of policies and procedures and adjustments to our goals and measurements.

Issue and Complaint Handling Process [33]

HSC provides a dedicated customer service desk for credentials verification services that allows customers, practitioners and third parties to contact us with questions, issues, or complaints regarding our processes.

Access is available 24/7 via email and phone, with the ability to leave messages after hours. The contact information for the customer service desk is posted on all our websites, on the request letters that we send out as part of the credentialing process and is provided to new customers as part of the onboarding process.

The customer service desk is staffed by two full time customer service representatives who handle most of the calls and the emails received daily to our dedicated phone line and mailbox. Our credentialing analysts provide coverage for the calls during the day via our hunt group capability to ensure that calls are handled promptly. Our goal is to resolve customer issues within 24 to 48 business hours. Calls and emails are handled in the order that they are received.

Our team make use of our companywide ticketing system, AutoTask, to log details of the calls and emails that are received throughout the day. If the frontline customer service team cannot resolve an issue immediately, the ticket will be assigned to the appropriate resource for resolution. Because our team of credentials analysts specialize and handle different aspects of the credentialing process, tickets are assigned to the appropriate analyst based on these responsibilities.

Within 1 business day of receipt of the email or call from the customer we will:

- Review the call or email received
- Identify the action or response required, where appropriate
- Perform the actions needed to address the item. If the item can be handled immediately, we will take the appropriate actions and communicate back to the customer with details of the resolution or steps that have been taken
- If research or escalation to an analyst is needed, a ticket will be assigned to the appropriate resource. We will then communicate to the customer to let them know that the issue has been reviewed and escalated to the appropriate resource for resolution

If an issue cannot be handled directly by our customer service team, the assigned analyst reviews the ticket, takes the appropriate steps to handle the ticket and will communicate to the customer and customer service team on the resolution of the issue. We aim to resolve most issues within 48 business hours. However, if more time is needed, we will communicate with the customer at regular intervals to

[33] CVO 2: Element B and Element C and Element D

keep them informed of progress, reach out for additional information, and give them an idea for when the issue will be resolved.

Depending on complexity, or the actions that need to be taken, not all issues can be resolved within 48 business hours. In the case of technical issues, such as application data issues, software issues, or items that may require development or programming from our Information Technology team, these tickets may be escalated internally to the IT help desk for resolution. Software issues may need to be added to the software development team's task list to be reviewed and prioritized based on urgency and resource availability. Tickets remain open until the issue is handled, whether in the credentialing queue in AutoTask or in the IT helpdesk queue in AutoTask for technical issues that require product fixes. Again, we let customers know the status of the resolution as progress is made. They can also check on the progress of issues at any time by contacting the customer service desk.

Through our system of cross training, we can cover the entire customer service process during times of high volume, and absences such as vacation time to ensure that we provide a consistently high level of service to our customers. On joining the team, new employees receive training on the customer service desk as part of their training plan and orientation to the department's activities. This involves a significant period shadowing the customer service representative to learn more about the types of calls and emails received and how they are handled, as well as specific training on the AutoTask ticketing system

Ticket Review Process

A selection of issue categories is built into AutoTask, specific to the credentials verification services department, and this allows us to monitor and trend the type and variety of issues being received over time. We are also able to track the time it takes for each issue to be resolved and this is one of the key indicators used to monitor the performance of the team.

The operations coordinator monitors the tickets received during the day to check for recurring issues or systemic problems that may have been reported and works closely with the customer service representatives. Urgent issues are immediately escalated to the program manager for resolution.

In addition, at the end of each month a report is generated from the ticketing system that summarizes all tickets received and completed during the month. This report is reviewed by the program manager each month to monitor any trends in issue categories that can feed into our ongoing quality improvement efforts.

In line with HSC's Five Customer Commitments, we aim to respond to customer requests timely and have a goal to resolve 94% of customer reported issues within 48 business hours. This monthly metric is tracked through AutoTask and is discussed with the credentials verification team during our regular Team meetings and huddles.

The customer service desk is not the only mechanism for collecting information on customer, practitioner, or third-party issues. Information on issues may also be received in the following ways:

- Customer relationship calls conducted by the program manager and senior credentials analyst as part of our companywide Customer Relationship Management initiative
- Routine follow up activities conducted by the program manager, operations coordinator, and credentials analysts as part of their daily core activities
- Feedback provided in comments submitted through Customer Satisfaction Surveys
- Feedback received during Customer Portal training for new customers or new credentialing staff joining an existing customer

Issues received from these sources will be logged and tracked in AutoTask as appropriate. Additionally, information gathered during these interactions and communications is used to validate current processes and to gather ideas for improvement and potential new services. This information is also shared with staff. Information on these items may be tracked within our ticketing system AutoTask which all team members have access to.

New customers are asked to complete a requirements questionnaire. This helps mitigate some of the customer issues experienced with new customers who are not accustomed to using a credentials verification organization. A clear outline of credentialing file requirements improves the communication between the credentials analysts and new customers as operational expectations are more clearly defined than in the contract language.

VIII. Protection of Credentialing Information[34]

HSC Security Policy[35]

HSC must treat as strictly confidential all credentials including, but not limited to, information from monitoring organizations that are not publicly available. Statements regarding confidentiality are featured prominently in our contracts with our customers. HSC recognizes that the release of such information to entities other than professional peer review and accrediting bodies may be prejudicial to the interests of the practitioner. HSC maintains a system to ensure the security and accuracy of the information it gathers, to provide its customers with valid data upon which to make decisions.

Implementation of the security policy and on-going attention to these issues are achieved by the organizational and departmental orientations, including training checklists and flex charts, emphasis on the importance of confidentiality, as documented by the signed confidentiality agreement, required staff training such as our annual HIPAA compliance training, cybersecurity training and on-going department level emphasis in daily interactions and staff meetings.

HSC values the following principles regarding confidentiality and security:

Maintenance of Confidential Information

All documentation obtained by HSC on behalf of the customer is considered confidential and is maintained in accordance with the confidentiality provisions of HCQIA, HIPAA, the applicable state's Review Organizational Immunity Act, and the applicable state's Medical Practices Act. The Credentials Verification Services Agreement specifies terms requiring confidentiality of information obtained.

Regarding HIPAA provisions, it is not the customary practice of the Staff Readiness/Credentialing Division of HSC to obtain information containing patient information. However, all credentials files have the potential to contain patient information as a result of the primary source verifications obtained by HSC on behalf of its customers. Such verifications include claims history verifications, licensure sanctions verifications, and National Practitioner Data Bank reports, among others. Due to this potential, all confidentiality and privacy provisions apply to patient information, as well as practitioner information. Patient information may not be disclosed in any manner except as specified by the contractual agreements and authorization releases HSC obtains prior to processing credentials verifications.

HSC may also gather information from the practitioner regarding his or her medical condition; however, this information is obtained through an authorization of release of information that was designed to meet HIPAA requirements.

[34] CVO 3
[35] CVO 3: Element A

Information obtained by HSC is preserved and maintained exclusively for the benefit of HSC's customers. The information will be duplicated and released to a third party only with the written consent of the applicant, pursuant to the Authorization, Attestation and Release (Release) form.

HSC will not release information to any customer unless the applicant has authorized this through a Release form. Additionally, if an applicant requests information contained in eCreds outside of the application form that they completed, HSC will instruct the requestor to contact the customer. HSC will not release any verification document to a non-customer. [36]

Upon hire, all new employees are given a thorough orientation to the security system and confidentiality procedures. This process is supported by the Policy and Procedure Manual, a one-on-one orientation and training, audits, the Confidentiality Statement, Employee Handbook and Orientation Checklist. All employees have a signed Confidentiality Statement in their personnel file, which is updated annually.[37]

The program manager thoroughly reviews all policies and procedures with all new employees during orientation, with particular attention focused on the confidentiality and security policies pertaining to credentials verifications.

All credentialing employees sign a statement on their training checklists stating they have received a thorough orientation as to their job responsibilities, and the confidentiality and security policies and procedures. This documents that all new employees have completed the orientation process, have reviewed all policies and procedures, and understand the significance of the confidentiality and security policies stipulated by the CVS policies and procedures.[38]

If an actual or potential organizational conflict of interest is identified during performance, HSC will immediately make a full disclosure in writing to the customer. A conflict-of-interest statement is obtained annually, as well, from all company employees.

Physical Access Control

Electronic credentials files (completed on or after June 12, 2012) are accessible through our secure, proprietary software application, eCreds. At the end of each business day, all staff computers are logged off. All external users are required to complete Access Authorization forms acknowledging their responsibilities in accessing confidential practitioner information.

HSC Domain security policies activate any logged in user's screen saver after 10 minutes of activity. The screen saver is password protected requiring a user to enter his or her domain password before continuing work. This applies to computers on site as well as any computers used to remotely access HSC systems. Any employees working remotely have a computer provided by HSC to be used exclusively for business purposes by the employee only. HSC networks and computers accessing the network are all continuously monitored for cybersecurity risks.[39]

Access to the server room is maintained by security code and the IT staff and human resources manager are the only authorized individuals with keys to this area.

Hard copy credentials files completed prior to June 12, 2012, are in a locked storage room, accessible by the program manager, customer service staff and the human resources manager. Hard copy files are retained for three years. Hard copies of verifications received by mail, email or fax are also

[36] CVO 3: Element A 2
[37] CVO 3: Element A 4
[38] CVO 3: Element A 5
[39] CVO 3: Element B 4

maintained in locked filing cabinets, accessible by the customer service staff and the manager. Hard copies of documents are purged within sixty days.

Visitors are required to sign in and out at the reception desk and are escorted by staff to areas beyond the lobby and ground floor meeting rooms.

The building's monitored security alarm system is automatically set every night at 10:30 p.m. Only current employees have the alarm code which activates and deactivates the building's security system. The alarm codes are changed periodically at the human resources manager's discretion.[40]

Personnel Management [41]

All new employees are given a thorough orientation to the details of the security rules and measures in place within the department and HSC.

Access to eCreds is limited to credentials verification, information technology and cross-trained staff and specific members of the management team. The ability to update, inactivate, and reorganize information in the eCreds program is limited to specific staff members with administrative rights.

Information is entered into eCreds if a hard copy application packet is received. Each document in the hard copy file is then scanned to the eCreds system, which then becomes the official receptacle of the hard copy file information. All hard copy and electronic documents are date stamped at the time of receipt. If telephone verification is done, the date of the verification is noted on the form used for the verification, and the party verifying the information is noted, as well as the name of the employee conducting the verification. This enables all verifications to be tracked according to when they were received and who received them so that it is very apparent which verifications are most current. This also establishes a historical tracking mechanism within each file since each document is date stamped. eCreds is then updated accordingly.

The eCreds software is an electronic storage mechanism of the hard copy file. The electronic file is the official information source and, therefore, the information contained in the eCreds is an accurate representation of the hard copy file. [42]

All employees are required to observe the company's Clean Desk Policy while handling any hard copy documents. This ensures all confidential documents are stored securely when not in use or when left unattended. Any hard copy confidential credentials documentation that can be discarded is placed in a secure container for shredding. All shred bins are locked so that documents cannot be accessed, and the documents are protected. We have a contract with a respected shredding vendor who regularly collect and dispose of the confidential information appropriately. Confidential information is material that includes any identifying information such as a physician's name, social security number, date of birth, registration/license numbers, or other similar personal data.[43]

Electronic Access and Monitoring Systems

The eCreds software application is password protected and accessible only to HSC employees who assist with the credentials verification process or respond to customer inquiries, information technology personnel, and specific members of our management team who need to access to specific reports.

Each authorized employee has a username and password for the eCreds software program in addition to network passwords, which are required to be changed every three months. Our network also employs

[40] CVO 3: Element B 5
[41] CVO 3: Element C
[42] CVO 3: Element B 2
[43] CVO 3: Element A 6

two factor authentication for additional security. Both eCreds and the network require strong passwords that are encrypted on the systems. Details of the users logged in are tracked and logged within eCreds. This allows us to monitor access to the system to ensure there is no unauthorized access. No changes to data can occur without being logged into the system as a designated user. A productivity report also tracks the tasks completed in real time and the name of the user completing the tasks. Again, this allows us to check for unauthorized access. Our IT department monitor access to our network as a whole to ensure no breaches or unauthorized access occurs.

The ability to print information and reports from eCreds is granted only to those staff members who have been issued a username and password. [44] If documents are to be discarded, they are flagged for shredding utilizing locked shred bins to protect the confidentiality of those documents.

HSC's domain security policies activate a screen saver after ten minutes of inactivity by a logged in user. The screen saver is password protected requiring the user to enter his or her domain password to access the network. This applies to computers used on site and computers provided for use remotely, off-site.[45]

Upon an employee's termination, an employee exit form is immediately completed by the program manager. This identifies all areas and programs the employee had access to, so that access to these systems can be revoked immediately on exit. The form is sent to our IT department and human resources manager, so network usernames and passwords are deactivated, as is their access to the building. Keys are also retrieved. The eCreds usernames and passwords are also removed. At the discretion of the human resources manager, the building alarm codes may also be changed.

Authorization to Modify Information [46]

HSC utilizes a role-based access control system. Each employee is provided access to the system with the minimum required permissions to do his or her job. Roles and access controls are monitored and changed, as appropriate.

The eCreds software application is password protected and accessible only to HSC employees who assist with the credentials verification process or respond to customer inquiries, information technology personnel, and specific members of our management team who need to access reports. Depending on the level of permission granted, users can modify certain types of data and reports that allow them to carry out their daily functions.

Permissions are set for each user when they join the organization, or when their role changes. The level of access they are granted to both the credentialing system and other areas of the organization is driven by the New Employee Onboarding Form which is completed and signed by the program manager.

A list of the key roles within the eCreds software is shown below:

- Administrator
- Applicant
- CanImpersonate
- Customer
- CVSAdmin
- CVSUser
- Practice Manager

[44] CVO 3, Element A, Factor 6
[45] CVO 3: Element B 4
[46] CVO 3: Element B 3

There are three levels of user permissions for internal users – CVSUser, CVSAdmin and Administrator. These user types can all view data in the system and modify data and documents within the limits of the screens they have access to and the available functionality on each screen. In addition, the CVSAdmin user has access to some additional reporting tools that the basic CVSUser role cannot access.

Only those with Administrator level access in the eCreds platform can modify user permissions and can deactivate information under the appropriate circumstances. The system does not allow information to be deleted. Instead, under the appropriate circumstances, for example, to remove erroneous or duplicate data or documentation, data and documents can be inactivated so that they do not impact the credentialing process. Inactivated items can still be viewed in the system and any audit trail related to those items can still be accessed.

Customers have very limited ability to update and edit information. This is limited to data relating to roster management, for example, changes to next reappointment dates and changes to practitioner contact information. When adding new providers to their roster via our Customer Portal, customers enter basic demographic information for the provider, such as name, title, date of birth (DOB), Social Security Number (SSN) and NPI number, as well as contact information. Once this data is entered to add the provider to the roster it cannot be changed by the customer. This data is ultimately verified against the application received from the practitioner – the application from the practitioner is the authoritative source of practitioner personal and professional information. Any discrepancies or typos made by the customer when entering the data can be reported to our customer service desk and changes can be made by a user with Administrator access, if appropriate. Details of these types of changes are tracked in our AutoTask ticketing system.

On receipt of an application from the practitioner, we ensure that the data provided in the customer request matches the data on the application by comparing the data within eCreds to the data on the application. This takes place during our Upload process or during the Input process. Any discrepancies in name, SSN or DOB must be investigated before changes are made to the data in eCreds. The ability to change this data is restricted to certain users who have the appropriate system access to change the data. These typically have CVSAdmin or Administrator level user accounts.

To track changes to these restricted data types, in July 2022, we added a new category into our AutoTask ticketing system to handle any identified data issues and track the steps taken to clarify and resolve these data discrepancies. Documentation supporting any changes that need to be made is saved to eCreds and will be included in any completed credentialling file to clearly identify the correct information.

HSC credentialing staff need to modify or update data when processing credentialing information received from providers and from third parties supplying primary source verification information. This is an essential function of their day-to-day activities. The data stored in eCreds must match the source of data which are saved as pdf documents in the system. The verification of the data against the credentialing documents gathered during the credentialing process is an essential component of the final audit of each and every file we complete. These documents are then combined into the completed credentialing file that is provided to customers on completion of the credentialing process.

Authorized users can modify information under the following circumstances:

- Update information during the credentialing or recredentialing cycle based on provider application information, including supporting documents and information from third party sources supplying primary source information

- Update information between credentialing cycles, for example, updates of expirable documents, or changes to demographic information such as contact information, changes of provider name or title. Provider name changes and changes of title can only be performed by those with CVSAdmin or Administrator level permissions to ensure integrity of data is maintained throughout the system. The change must be supported by documentation
- Remove erroneous or duplicate data, or documentation that impacts the credentialing process
- Inactivate retired or deceased providers to ensure that no credentialing activity happens on their behalf. Inactivation of providers is strictly limited to those who have Administrator level access. Provider records are never deleted
- Documentation received from practitioners, customers and third parties that may prompt changes in the system such as name or title changes, or other demographic changes, such as address changes are saved in the system to ensure that documentation exists to indicate why certain data has been updated

Monitoring Access and Tracking Changes [47]

As mentioned above, logging tables in eCreds allow us to see which users have logged into the system. Changes to data can only be made by a user who is logged in. Productivity reports also show the tasks completed by each user. The productivity report is monitored throughout the day by the Operations Coordinator to ensure only authorized personnel are working in the system. At the end of each month, the figures for the month are summarized and sent to the program manager to review. This allows us to confirm that only authorized users are working in the system.

eCreds tracks activity of specific system queues, including dates tasks were worked and completed, dates data records were created and modified and the name of the user performing the activity tracked. Queries of these tables allow us to ensure that data is only modified by authorized users. Data cannot be changed without logging into the system. While the tracking of the exact change made is not yet automated, all data can be tracked back to either an application we have received, a supporting document or verification received during the credentialing process. Until we automate, we have a procedure in place to document and track any data modification (see below). Additionally, we audit credentialing files daily to verify that data matches the source documents and to check for consistency of restricted data like name, DOB and SSN with previous applications received.

As part of our 15-day file review process and during the final audit of each credentialing file, an analyst compares the data saved in eCreds against the pdf documents saved in the system which are the authoritative source of the system data. This includes the review of any supporting documentation for name changes and modifications to other restricted data elements such as practitioner name, DOB and SSN. Files will not pass audit and be shipped to customers if discrepancies exist in data or there are changes to data that are not supported by documentation.

In 2023, as part of HSC's Cyber Security initiative which was identified and prioritized as part of the 2022 strategic planning process, additional logging will be added to eCreds. These changes will allow us to track in real-time modifications to restricted data elements such as practitioner name, SSN and DOB to ensure they have been made in line with our policies and procedures. Similarly, we will be able to detect task activity performed by unauthorized users.

Until that time, we monitor data modifications through the following methods:

- Daily, through comparison of received documents against the data stored in eCreds during document processing in our electronic mailroom, application processing at input and upload, our

[47] CVO 3: Element B 6

audit process and 15-day file review process. At audit and during the 15-day file review, credentialing data and restricted data elements relevant to the file are reviewed to make sure that they match documents received and stored in the system and make comparisons to documents received at the prior credentialing cycle, if applicable. This also happens as applications are received at input and upload and are linked to a specific practitioner in our system

- Daily, through handling of AutoTask tickets under the data changes category
- Monthly through a review of AutoTask tickets handled under the data changes category to ensure that all non-standard data changes are tracked appropriately and that the appropriate actions and levels of documentation have been saved to the system
- As part of our monthly sample audit of files, we have always reviewed the restricted data elements and make sure that they match documents received and stored in the system and are compared to documents received at the prior credentialing cycle, if applicable
- Review of credential data saved in eCreds tables to ensure changes are only made by authorized users at least twice a year. This reinforces the monthly monitoring of log in activity and queue activity that has been in place for many years

Business Continuity/Disaster Recovery/Data Integrity [48]

HSC's business continuity and disaster recovery plan addresses procedures for ensuring the continuity of the business in the case of an emergency or disaster that requires adjustments to normal business activities for a prolonged period of time. The focus is on restoration of customer operations. Alternative work arrangements include employees working from home, on alternative schedules, and/or at a separate facility.

HSC has several security/preventive measures, technical redundancies, and back-up procedures, as follows:

- All employees are required to read and attest to the HSC Acceptable Use Policy, the Confidentiality Agreement, The HSC Business Ethics Code, and HSC Staff Readiness/Credentialing employees are required to learn and attest to the Data Governance for Credentialing policy
- HSC has a firewall deployed to protect our network against external threats.
- HSC requires multi-factor authentication.
- HSC performs an annual independent vulnerability scan and assessment to verify that our network and computer systems are properly protected from external attacks. HSC uses ESET antivirus and all of our inbound and outbound emails are filtered by Office 365 Exchange Security for potential viruses and threats.
- All authorized external access to the internal HSC system is through a secure encrypted VPN access.
- All computer hardware is issued and monitored by HSC IT. All access to our web based services, internal and external, is protected through use of Secure Socket Layer (SSL). There is no access to the system using an unsecured transfer protocol.
- Customer access to completed files is protected by role based security, as well as SSL encryption during the downloading of documents.
- HSC deploys the concept of "least privilege" in our network and computer system security model utilizing security groups in our windows active directory structure. All additions, changes, or deletions of user accounts and user access are initiated using a form completed by the applicable business unit manager and verify by the Information Technology Department.

[48] CVO 3: Element D

- HSC utilizes Team Foundation Server 2015 for our production program source and revision control.
- HSC has deployed a network monitoring system that will alert for the following: computer room power, CPU utilization, SQL Server DB health, IIS services, Exchange services, scheduled tasks, event, system, and application log monitoring, and FTP/HTTP. When triggered, the system will alert the emergency response team for appropriate action. Any significant outage or issue will be escalated based on established policies and procedures.
- HSC utilizes computer room temperature sensors that will monitor for the appropriate temperature and alert IT staff through text or email messages.
- HSC's building is locked 24/7 and has radio frequency identifier card controlled access.
- HSC's server room is locked 24/7 and can only be accessed by authorized staff. All access by non-IT personnel is logged.
- HSC performs daily back-up of all servers and data. Full back-ups are taken to an offsite data center that is environmentally protected. Weekly, all data and applications are fully backed up, and incremental and/or differential backups are performed each evening.
- HSC also maintains off-site documentation of all server configurations in an off-site accessible location.
- HSC has redundancy protection in the following areas:
    - Uninterrupted power supply devices providing power to the servers, configured to bring down non-essential services in the event of a power outage to ensure essential services are operational for longer periods.
    - A virtual system with fail-over capabilities. Servers are paired and split between hosts to provide continued operations when a system becomes unavailable.
    - Two computer room cooling units are deployed with one acting as a fail-over in the event of a failure of the primary chiller. A third, off-line, spare cooling unit can be immediately deployed, if necessary.

HSC employs a "3-2-1" backup strategy with three copies of data – two local backups on different media, and a copy off-site. In the event of a system crash, the information contained in the eCreds software program will not be lost. This backup runs on a nightly basis. HSC uses a disk-based backup method with a rolling archive system. Weekly, each server has a full backup and daily, an incremental backup is performed. Database servers perform a full backup weekly and a differential backup nightly. Transaction logs are backed up nightly. The backup status is monitored daily and any issues are addressed immediately. The backup system processes are reviewed and tested annually.

In the event of a power failure, the server will continue to operate on an uninterrupted power supply, enabling staff to safely shut it down within a sufficient amount of time without damaging the integrity of the program or data.

On-Line Access

Customer Portal

The Customer Portal allows customers to view their practitioner files in eCreds for status queries and multiple reporting capabilities 24 hours a day, 7 days a week.

Before being granted access to the portal, each customer contact completes an On-line Access User Request Form and submits it to HSC. No user is granted access to the system without completing a request form. When access is granted to the customer contact, a username and password is assigned. The customer contact then creates a new string password that is encrypted in the system. A password reset feature is available if the customer contact should forget his or her password.

The Customer Portal provides a robust set of security and audit controls. This service only allows the customer to view a subset of the information contained in eCreds. Each relevant piece of information is represented by an “Information Rule” that is executed to retrieve or update the information. Each Information Rule has an Access Control List associated with it that explicitly defines which individual user or groups of users are allowed to execute the rule. If a user is not allowed to run the Information Rule, that information is simply not available or displayed to that user.

The following outline represents the security measures employed by the Customer Portal:

- Isolated network using a state-of-the-art firewall software.
- Encryption - Front-end: Secure Sockets Layer (SSL) between the user’s web browser and the application server.
- Encryption – Back-end: ISAPI/NSAPI plug-in between Web Server, and the application server.
- Authentication: installed network authentication and other security controls.
- Security: server and platforms in a controlled locked area (cool-room).
- MS Windows 2008 Operating System – the configuration eliminates operating system weaknesses through procedure and administration.
- MS Windows 2012 Operating System network Active Directory and user level security.

There are several security and access levels based on a user’s membership in a group (i.e., the Administrative Services level or the Client Services level). The service currently uses a basic system of user ID and passwords to authenticate users. The service administrator(s) may also assign users to one or more group and then control access based on the group name rather than an individual user ID. This helps categorize groups in a “role-based” manner to track access by group.

Practitioner Portal

Utilizing the same secure methods as for the Customer Portal, HSC has developed a completely automated on-line credentials application. Practitioners and their practice managers are directed to our secure website and allowed to create a password and ID to log in and complete the application process. If the practitioner is or has been credentialed by HSC previously, the application is pre-populated based upon the latest available data in the system. Once a practitioner has completed the on-line application, it is submitted to HSC for processing.

Prepopulation of the application with data stored in eCreds only happens if the preliminary data entered at the beginning of the application process matches the data in eCreds. This data is comprised of four data elements – last name, first name, DOB and SSN. Only if the data is an exact match to the data in eCreds will prepopulation occur. This restriction prevents authenticated system data from being overwritten by new data which may not be correct, due to errors or typos. Once submitted, data from the online application is reviewed and uploaded into eCreds, during the upload process. If an application was not prepopulated, we check to see if the provider is in the system already and data will be loaded if appropriate if we can verify that the provider is one and the same. Even if the data is added new to the system because of a data mismatch eventually the two provider records will be identified as a common provider and following a resolution of data discrepancies the data will be merged. This is known in our system as a duplicate DocCode, and these types of resolution are tracked in AutoTask and can only be handled and resolved by a user with Administrator level access.

IX. CVS Policy Changes [49]

The policies and procedures for CVS are reviewed and updated by the manager no less than annually and are kept current according to Joint Commission and NCQA standards. All policy changes are communicated to staff formally in staff meetings and informally during day-to-day communications.

Annual Review

The manager conducts (at a minimum) a bi-annual review of the CVS Policies and Procedures. Any revised documents are presented to the President/CEO for review and approval. Upon approval by the President/CEO, the revised policies and procedures are distributed to the appropriate staff members and customers. All outdated policies and procedures are archived in the “Archived P & P’s” electronic folder.

Interim and On-Going Review

The manager and analysts continually monitor the Joint Commission and NCQA regulations and guidelines, as changes become available, to ensure all policies and procedures are updated and implemented accordingly. As improvement areas are identified, the manager revises the policies and procedures in order to implement quality control activities in a timely manner. These changes are then incorporated into the policies and procedures current revision file. They are communicated internally during daily huddles and/or communicated and reinforced during staff meetings. They are also communicated externally, as necessary.

X. Delegation of CVO Activities [50]

HSC does not delegate any NCQA-required credentialing activities. Because no activities are delegated there is nothing that requires oversight.

[49] CVO 1: Element A. 7.

[50] CVO 15