Department of Administration
Purchasing Division
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

State of West Virginia
Master Agreement

Order Date: 03-11-2024

CORRECT ORDER NUMBER MUST APPEAR ON ALL PACKAGES, INVOICES, AND SHIPPING PAPERS. QUESTIONS CONCERNING THIS ORDER SHOULD BE DIRECTED TO THE DEPARTMENT CONTACT.

Order Number:	CMA 0506 2820 MIS2400000002 1	**Procurement Folder:**	1368793
Document Name:	HOSPITAL INPATIENT DATA SYSTEM (HIDS)	**Reason for Modification:**	
Document Description:	HOSPITAL INPATIENT DATA SYSTEM (HIDS)		
Procurement Type:	Central Master Agreement		
Buyer Name:			
Telephone:			
Email:			
Shipping Method:	Best Way	**Effective Start Date:**	2024-04-01
Free on Board:	FOB Dest, Freight Prepaid	**Effective End Date:**	2025-03-31

VENDOR

Vendor Customer Code: 000000200474
WV HOSPITAL ASSOC
100 ASSOCIATION DR

CHARLESTON WV 25311-1571
US
Vendor Contact Phone: 304-353-9724 **Extension:**

Discount Details:

	Discount Allowed	Discount Percentage	Discount Days
#1	No	0.0000	0
#2	No		
#3	No		
#4	No		

DEPARTMENT CONTACT

Requestor Name: Stephanie F Pettry
Requestor Phone: (304) 356-4011
Requestor Email: stephanie.f.pettry@wv.gov

24
FILE LOCATION_____

INVOICE TO

PROCUREMENT OFFICER
HEALTH CARE AUTHORITY

100 DEE DR

CHARLESTON WV 25311-1692

US

SHIP TO

HEALTH INFORMATION NETWORK CFO
HEALTH CARE AUTHORITY / HEALTH INFORMATION NETWORK

100 DEE DR

CHARLESTON WV 25311-1692

US

3-13-24 GL

Purchasing Division's File Copy

Total Order Amount:	Open End

CH 3/11/24

PURCHASING DIVISION AUTHORIZATION	ATTORNEY GENERAL APPROVAL AS TO FORM	ENCUMBRANCE CERTIFICATION
DATE: Tiffany 3/12/2024	DATE: John S. Gray 3/18/2024	DATE: Jay 3-18-24
ELECTRONIC SIGNATURE ON FILE	ELECTRONIC SIGNATURE ON FILE	ELECTRONIC SIGNATURE ON FILE

Extended Description:

THE VENDOR, WEST VIRGINIA HOSPITAL ASSOCIATION, AGREES TO ENTER WITH THE AGENCY, WEST VIRGINIA DEPARTMENT OF HEALTH AND HUMAN RESOURCES, OFFICE OF SHARED ADMINISTRATION FOR THE WV HEALTH CARE AUTHORITY (HCA), INTO AN OPEN-END CONTRACT TO UPGRADE OR REPLACE THE EXISTING HOSPITAL INPATIENT DATA SYSTEM (HIDS) PER THE TERMS AND CONDITIONS, SPECIFICATIONS, BID REQUIREMENTS, AND THE VENDOR'S BID DATED 02/26/2024, INCORPORATED HEREIN BY REFERENCE, AND MADE A PART OF HEREOF.

Line	Commodity Code	Manufacturer	Model No	Unit	Unit Price
1	81111503			QTR	65497.000000
	Service From	**Service To**		**Service Contract Amount**	
				0.00	

Commodity Line Description: Base System- HUBDS

Extended Description:
Base System- Hospital UB Data System (HUBDS)

Line	Commodity Code	Manufacturer	Model No	Unit	Unit Price
2	81111503			QTR	20500.000000
	Service From	**Service To**		**Service Contract Amount**	
				0.00	

Commodity Line Description: Additional Optional System Module

Extended Description:
Additional Optional System Module (3.1.3.2.11)

Line	Commodity Code	Manufacturer	Model No	Unit	Unit Price
3	81111503			HOUR	2.000000
	Service From	**Service To**		**Service Contract Amount**	
				0.00	

Commodity Line Description: Optional Services

Extended Description:
Optional Services (3.1.8)
Hourly Rate for all optional services

GENERAL TERMS AND CONDITIONS:

1. CONTRACTUAL AGREEMENT: Issuance of an Award Document signed by the Purchasing Division Director, or his designee, and approved as to form by the Attorney General's office constitutes acceptance by the State of this Contract made by and between the State of West Virginia and the Vendor. Vendor's signature on its bid, or on the Contract if the Contract is not the result of a bid solicitation, signifies Vendor's agreement to be bound by and accept the terms and conditions contained in this Contract.

2. DEFINITIONS: As used in this Solicitation/Contract, the following terms shall have the meanings attributed to them below. Additional definitions may be found in the specifications included with this Solicitation/Contract.

2.1. "Agency" or **"Agencies"** means the agency, board, commission, or other entity of the State of West Virginia that is identified on the first page of the Solicitation or any other public entity seeking to procure goods or services under this Contract.

2.2. "Bid" or **"Proposal"** means the vendors submitted response to this solicitation.

2.3. "Contract" means the binding agreement that is entered into between the State and the Vendor to provide the goods or services requested in the Solicitation.

2.4. "Director" means the Director of the West Virginia Department of Administration, Purchasing Division.

2.5. "Purchasing Division" means the West Virginia Department of Administration, Purchasing Division.

2.6. "Award Document" means the document signed by the Agency and the Purchasing Division, and approved as to form by the Attorney General, that identifies the Vendor as the contract holder.

2.7. "Solicitation" means the official notice of an opportunity to supply the State with goods or services that is published by the Purchasing Division.

2.8. "State" means the State of West Virginia and/or any of its agencies, commissions, boards, etc. as context requires.

2.9. "Vendor" or **"Vendors"** means any entity submitting a bid in response to the Solicitation, the entity that has been selected as the lowest responsible bidder, or the entity that has been awarded the Contract as context requires.

3. CONTRACT TERM; RENEWAL; EXTENSION: The term of this Contract shall be determined in accordance with the category that has been identified as applicable to this Contract below:

☑ **Term Contract**

Initial Contract Term: The Initial Contract Term will be for a period of one (1) year. The Initial Contract Term becomes effective on the effective start date listed on the first page of this Contract, identified as the State of West Virginia contract cover page containing the signatures of the Purchasing Division, Attorney General, and Encumbrance clerk (or another page identified as _____), and the Initial Contract Term ends on the effective end date also shown on the first page of this Contract.

Renewal Term: This Contract may be renewed upon the mutual written consent of the Agency, and the Vendor, with approval of the Purchasing Division and the Attorney General's office (Attorney General approval is as to form only). Any request for renewal should be delivered to the Agency and then submitted to the Purchasing Division thirty (30) days prior to the expiration date of the initial contract term or appropriate renewal term. A Contract renewal shall be in accordance with the terms and conditions of the original contract. Unless otherwise specified below, renewal of this Contract is limited to three (3) successive one (1) year periods or multiple renewal periods of less than one year, provided that the multiple renewal periods do not exceed the total number of months available in all renewal years combined. Automatic renewal of this Contract is prohibited. Renewals must be approved by the Vendor, Agency, Purchasing Division and Attorney General's office (Attorney General approval is as to form only)

☐ **Alternate Renewal Term** – This contract may be renewed for _____ successive _____ year periods or shorter periods provided that they do not exceed the total number of months contained in all available renewals. Automatic renewal of this Contract is prohibited. Renewals must be approved by the Vendor, Agency, Purchasing Division and Attorney General's office (Attorney General approval is as to form only)

Delivery Order Limitations: In the event that this contract permits delivery orders, a delivery order may only be issued during the time this Contract is in effect. Any delivery order issued within one year of the expiration of this Contract shall be effective for one year from the date the delivery order is issued. No delivery order may be extended beyond one year after this Contract has expired.

☐ **Fixed Period Contract:** This Contract becomes effective upon Vendor's receipt of the notice to proceed and must be completed within _____ days.

☐ **Fixed Period Contract with Renewals:** This Contract becomes effective upon Vendor's receipt of the notice to proceed and part of the Contract more fully described in the attached specifications must be completed within _____ days. Upon completion of the work covered by the preceding sentence, the vendor agrees that:

☐ the contract will continue for _____ years;

☐ the contract may be renewed for _____ successive _____ year periods or shorter periods provided that they do not exceed the total number of months contained in all available renewals. Automatic renewal of this Contract is prohibited. Renewals must be approved by the Vendor, Agency, Purchasing Division and Attorney General's Office (Attorney General approval is as to form only).

☐ **One-Time Purchase:** The term of this Contract shall run from the issuance of the Award Document until all of the goods contracted for have been delivered, but in no event will this Contract extend for more than one fiscal year.

☐ **Construction/Project Oversight:** This Contract becomes effective on the effective start date listed on the first page of this Contract, identified as the State of West Virginia contract cover page containing the signatures of the Purchasing Division, Attorney General, and Encumbrance clerk (or another page identified as _____), and continues until the project for which the vendor is providing oversight is complete.

☐ **Other:** Contract Term specified in _____

4. AUTHORITY TO PROCEED: Vendor is authorized to begin performance of this contract on the date of encumbrance listed on the front page of the Award Document unless either the box for "Fixed Period Contract" or "Fixed Period Contract with Renewals" has been checked in Section 3 above. If either "Fixed Period Contract" or "Fixed Period Contract with Renewals" has been checked, Vendor must not begin work until it receives a separate notice to proceed from the State. The notice to proceed will then be incorporated into the Contract via change order to memorialize the official date that work commenced.

5. QUANTITIES: The quantities required under this Contract shall be determined in accordance with the category that has been identified as applicable to this Contract below.

☑ **Open End Contract:** Quantities listed in this Solicitation/Award Document are approximations only, based on estimates supplied by the Agency. It is understood and agreed that the Contract shall cover the quantities actually ordered for delivery during the term of the Contract, whether more or less than the quantities shown.

☐ **Service:** The scope of the service to be provided will be more clearly defined in the specifications included herewith.

☐ **Combined Service and Goods:** The scope of the service and deliverable goods to be provided will be more clearly defined in the specifications included herewith.

☐ **One-Time Purchase:** This Contract is for the purchase of a set quantity of goods that are identified in the specifications included herewith. Once those items have been delivered, no additional goods may be procured under this Contract without an appropriate change order approved by the Vendor, Agency, Purchasing Division, and Attorney General's office.

☐ **Construction:** This Contract is for construction activity more fully defined in the specifications.

6. EMERGENCY PURCHASES: The Purchasing Division Director may authorize the Agency to purchase goods or services in the open market that Vendor would otherwise provide under this Contract if those goods or services are for immediate or expedited delivery in an emergency. Emergencies shall include, but are not limited to, delays in transportation or an unanticipated increase in the volume of work. An emergency purchase in the open market, approved by the Purchasing Division Director, shall not constitute of breach of this Contract and shall not entitle the Vendor to any form of compensation or damages. This provision does not excuse the State from fulfilling its obligations under a One-Time Purchase contract.

7. REQUIRED DOCUMENTS: All of the items checked in this section must be provided to the Purchasing Division by the Vendor as specified:

☐ **LICENSE(S) / CERTIFICATIONS / PERMITS:** In addition to anything required under the Section of the General Terms and Conditions entitled Licensing, the apparent successful Vendor shall furnish proof of the following licenses, certifications, and/or permits upon request and in a form acceptable to the State. The request may be prior to or after contract award at the State's sole discretion.

☐ N/A

☐

☐

☐

The apparent successful Vendor shall also furnish proof of any additional licenses or certifications contained in the specifications regardless of whether or not that requirement is listed above.

8. INSURANCE: The apparent successful Vendor shall furnish proof of the insurance identified by a checkmark below prior to Contract award. The insurance coverages identified below must be maintained throughout the life of this contract. Thirty (30) days prior to the expiration of the insurance policies, Vendor shall provide the Agency with proof that the insurance mandated herein has been continued. Vendor must also provide Agency with immediate notice of any changes in its insurance policies, including but not limited to, policy cancelation, policy reduction, or change in insurers. The apparent successful Vendor shall also furnish proof of any additional insurance requirements contained in the specifications prior to Contract award regardless of whether that insurance requirement is listed in this section.

Vendor must maintain:

☑ **Commercial General Liability Insurance** in at least an amount of: $1,000,000.00 per occurrence.

☐ **Automobile Liability Insurance** in at least an amount of: _____ per occurrence.

☐ **Professional/Malpractice/Errors and Omission Insurance** in at least an amount of: _____ per occurrence. Notwithstanding the forgoing, Vendor's are not required to list the State as an additional insured for this type of policy.

☐ **Commercial Crime and Third Party Fidelity Insurance** in an amount of: _____ per occurrence.

☐ **Cyber Liability Insurance** in an amount of: _____ per occurrence.

☐ **Builders Risk Insurance** in an amount equal to 100% of the amount of the Contract.

☐ **Pollution Insurance** in an amount of: _____ per occurrence.

☐ **Aircraft Liability** in an amount of: _____ per occurrence.

☐

☐

☐

☐

9. WORKERS' COMPENSATION INSURANCE: Vendor shall comply with laws relating to workers compensation, shall maintain workers' compensation insurance when required, and shall furnish proof of workers' compensation insurance upon request.

10. VENUE: All legal actions for damages brought by Vendor against the State shall be brought in the West Virginia Claims Commission. Other causes of action must be brought in the West Virginia court authorized by statute to exercise jurisdiction over it.

11. LIQUIDATED DAMAGES: This clause shall in no way be considered exclusive and shall not limit the State or Agency's right to pursue any other available remedy. Vendor shall pay liquidated damages in the amount specified below or as described in the specifications:

☐ N/A _____ for _____.

☐ Liquidated Damages Contained in the Specifications.

☐ Liquidated Damages Are Not Included in this Contract.

12. ACCEPTANCE: Vendor's signature on its bid, or on the certification and signature page, constitutes an offer to the State that cannot be unilaterally withdrawn, signifies that the product or service proposed by vendor meets the mandatory requirements contained in the Solicitation for that product or service, unless otherwise indicated, and signifies acceptance of the terms and conditions contained in the Solicitation unless otherwise indicated.

13. PRICING: The pricing set forth herein is firm for the life of the Contract, unless specified elsewhere within this Solicitation/Contract by the State. A Vendor's inclusion of price adjustment provisions in its bid, without an express authorization from the State in the Solicitation to do so, may result in bid disqualification. Notwithstanding the foregoing, Vendor must extend any publicly advertised sale price to the State and invoice at the lower of the contract price or the publicly advertised sale price.

14. PAYMENT IN ARREARS: Payments for goods/services will be made in arrears only upon receipt of a proper invoice, detailing the goods/services provided or receipt of the goods/services, whichever is later. Notwithstanding the foregoing, payments for software maintenance, licenses, or subscriptions may be paid annually in advance.

15. PAYMENT METHODS: Vendor must accept payment by electronic funds transfer and P-Card. (The State of West Virginia's Purchasing Card program, administered under contract by a banking institution, processes payment for goods and services through state designated credit cards.)

16. TAXES: The Vendor shall pay any applicable sales, use, personal property or any other taxes arising out of this Contract and the transactions contemplated thereby. The State of West Virginia is exempt from federal and state taxes and will not pay or reimburse such taxes.

17. ADDITIONAL FEES: Vendor is not permitted to charge additional fees or assess additional charges that were not either expressly provided for in the solicitation published by the State of West Virginia, included in the Contract, or included in the unit price or lump sum bid amount that Vendor is required by the solicitation to provide. Including such fees or charges as notes to the solicitation may result in rejection of vendor's bid. Requesting such fees or charges be paid after the contract has been awarded may result in cancellation of the contract.

18. FUNDING: This Contract shall continue for the term stated herein, contingent upon funds being appropriated by the Legislature or otherwise being made available. In the event funds are not appropriated or otherwise made available, this Contract becomes void and of no effect beginning on July 1 of the fiscal year for which funding has not been appropriated or otherwise made available. If that occurs, the State may notify the Vendor that an alternative source of funding has been obtained and thereby avoid the automatic termination. Non-appropriation or non-funding shall not be considered an event of default.

19. CANCELLATION: The Purchasing Division Director reserves the right to cancel this Contract immediately upon written notice to the vendor if the materials or workmanship supplied do not conform to the specifications contained in the Contract. The Purchasing Division Director may also cancel any purchase or Contract upon 30 days written notice to the Vendor in accordance with West Virginia Code of State Rules § 148-1-5.2.b.

20. TIME: Time is of the essence regarding all matters of time and performance in this Contract.

21. APPLICABLE LAW: This Contract is governed by and interpreted under West Virginia law without giving effect to its choice of law principles. Any information provided in specification manuals, or any other source, verbal or written, which contradicts or violates the West Virginia Constitution, West Virginia Code, or West Virginia Code of State Rules is void and of no effect.

22. COMPLIANCE WITH LAWS: Vendor shall comply with all applicable federal, state, and local laws, regulations and ordinances. By submitting a bid, Vendor acknowledges that it has reviewed, understands, and will comply with all applicable laws, regulations, and ordinances.

> **SUBCONTRACTOR COMPLIANCE:** Vendor shall notify all subcontractors providing commodities or services related to this Contract that as subcontractors, they too are required to comply with all applicable laws, regulations, and ordinances. Notification under this provision must occur prior to the performance of any work under the contract by the subcontractor.

23. ARBITRATION: Any references made to arbitration contained in this Contract, Vendor's bid, or in any American Institute of Architects documents pertaining to this Contract are hereby deleted, void, and of no effect.

24. MODIFICATIONS: This writing is the parties' final expression of intent. Notwithstanding anything contained in this Contract to the contrary no modification of this Contract shall be binding without mutual written consent of the Agency, and the Vendor, with approval of the Purchasing Division and the Attorney General's office (Attorney General approval is as to form only). Any change to existing contracts that adds work or changes contract cost, and were not included in the original contract, must be approved by the Purchasing Division and the Attorney General's Office (as to form) prior to the implementation of the change or commencement of work affected by the change.

25. WAIVER: The failure of either party to insist upon a strict performance of any of the terms or provision of this Contract, or to exercise any option, right, or remedy herein contained, shall not be construed as a waiver or a relinquishment for the future of such term, provision, option, right, or remedy, but the same shall continue in full force and effect. Any waiver must be expressly stated in writing and signed by the waiving party.

26. SUBSEQUENT FORMS: The terms and conditions contained in this Contract shall supersede any and all subsequent terms and conditions which may appear on any form documents submitted by Vendor to the Agency or Purchasing Division such as price lists, order forms, invoices, sales agreements, or maintenance agreements, and includes internet websites or other electronic documents. Acceptance or use of Vendor's forms does not constitute acceptance of the terms and conditions contained thereon.

27. ASSIGNMENT: Neither this Contract nor any monies due, or to become due hereunder, may be assigned by the Vendor without the express written consent of the Agency, the Purchasing Division, the Attorney General's office (as to form only), and any other government agency or office that may be required to approve such assignments.

28. WARRANTY: The Vendor expressly warrants that the goods and/or services covered by this Contract will: (a) conform to the specifications, drawings, samples, or other description furnished or specified by the Agency; (b) be merchantable and fit for the purpose intended; and (c) be free from defect in material and workmanship.

29. STATE EMPLOYEES: State employees are not permitted to utilize this Contract for personal use and the Vendor is prohibited from permitting or facilitating the same.

30. PRIVACY, SECURITY, AND CONFIDENTIALITY: The Vendor agrees that it will not disclose to anyone, directly or indirectly, any such personally identifiable information or other confidential information gained from the Agency, unless the individual who is the subject of the information consents to the disclosure in writing or the disclosure is made pursuant to the Agency's policies, procedures, and rules. Vendor further agrees to comply with the Confidentiality Policies and Information Security Accountability Requirements, set forth in www.state.wv.us/admin/purchase/privacy.

31. YOUR SUBMISSION IS A PUBLIC DOCUMENT: Vendor's entire response to the Solicitation and the resulting Contract are public documents. As public documents, they will be disclosed to the public following the bid/proposal opening or award of the contract, as required by the competitive bidding laws of West Virginia Code §§ 5A-3-1 et seq., 5-22-1 et seq., and 5G-1-1 et seq. and the Freedom of Information Act West Virginia Code §§ 29B-1-1 et seq.

DO NOT SUBMIT MATERIAL YOU CONSIDER TO BE CONFIDENTIAL, A TRADE SECRET, OR OTHERWISE NOT SUBJECT TO PUBLIC DISCLOSURE.

Submission of any bid, proposal, or other document to the Purchasing Division constitutes your explicit consent to the subsequent public disclosure of the bid, proposal, or document. The Purchasing Division will disclose any document labeled "confidential," "proprietary," "trade secret," "private," or labeled with any other claim against public disclosure of the documents, to include any "trade secrets" as defined by West Virginia Code § 47-22-1 et seq. All submissions are subject to public disclosure without notice.

32. LICENSING: In accordance with West Virginia Code of State Rules § 148-1-6.1.e, Vendor must be licensed and in good standing in accordance with any and all state and local laws and requirements by any state or local agency of West Virginia, including, but not limited to, the West Virginia Secretary of State's Office, the West Virginia Tax Department, West Virginia Insurance Commission, or any other state agency or political subdivision. Obligations related to political subdivisions may include, but are not limited to, business licensing, business and occupation taxes, inspection compliance, permitting, etc. Upon request, the Vendor must provide all necessary releases to obtain information to enable the Purchasing Division Director or the Agency to verify that the Vendor is licensed and in good standing with the above entities.

SUBCONTRACTOR COMPLIANCE: Vendor shall notify all subcontractors providing commodities or services related to this Contract that as subcontractors, they too are required to be licensed, in good standing, and up-to-date on all state and local obligations as described in this section. Obligations related to political subdivisions may include, but are not limited to, business licensing, business and occupation taxes, inspection compliance, permitting, etc. Notification under this provision must occur prior to the performance of any work under the contract by the subcontractor.

33. ANTITRUST: In submitting a bid to, signing a contract with, or accepting a Award Document from any agency of the State of West Virginia, the Vendor agrees to convey, sell, assign, or transfer to the State of West Virginia all rights, title, and interest in and to all causes of action it may now or hereafter acquire under the antitrust laws of the United States and the State of West Virginia for price fixing and/or unreasonable restraints of trade relating to the particular commodities or services purchased or acquired by the State of West Virginia. Such assignment shall be made and become effective at the time the purchasing agency tenders the initial payment to Vendor.

34. VENDOR NON-CONFLICT: Neither Vendor nor its representatives are permitted to have any interest, nor shall they acquire any interest, direct or indirect, which would compromise the performance of its services hereunder. Any such interests shall be promptly presented in detail to the Agency.

35. VENDOR RELATIONSHIP: The relationship of the Vendor to the State shall be that of an independent contractor and no principal-agent relationship or employer-employee relationship is contemplated or created by this Contract. The Vendor as an independent contractor is solely liable for the acts and omissions of its employees and agents. Vendor shall be responsible for selecting, supervising, and compensating any and all individuals employed pursuant to the terms of this Solicitation and resulting contract. Neither the Vendor, nor any employees or subcontractors of the Vendor, shall be deemed to be employees of the State for any purpose whatsoever. Vendor shall be exclusively responsible for payment of employees and contractors for all wages and salaries, taxes, withholding payments, penalties, fees, fringe benefits, professional liability insurance premiums, contributions to insurance and pension, or other deferred compensation plans, including but not limited to, Workers' Compensation and Social Security obligations, licensing fees, etc. and the filing of all necessary documents, forms, and returns pertinent to all of the foregoing.

Vendor shall hold harmless the State, and shall provide the State and Agency with a defense against any and all claims including, but not limited to, the foregoing payments, withholdings, contributions, taxes, Social Security taxes, and employer income tax returns.

36. INDEMNIFICATION: The Vendor agrees to indemnify, defend, and hold harmless the State and the Agency, their officers, and employees from and against: (1) Any claims or losses for services rendered by any subcontractor, person, or firm performing or supplying services, materials, or supplies in connection with the performance of the Contract; (2) Any claims or losses resulting to any person or entity injured or damaged by the Vendor, its officers, employees, or subcontractors by the publication, translation, reproduction, delivery, performance, use, or disposition of any data used under the Contract in a manner not authorized by the Contract, or by Federal or State statutes or regulations; and (3) Any failure of the Vendor, its officers, employees, or subcontractors to observe State and Federal laws including, but not limited to, labor and wage and hour laws.

37. NO DEBT CERTIFICATION: In accordance with West Virginia Code §§ 5A-3-10a and 5-22-1(i), the State is prohibited from awarding a contract to any bidder that owes a debt to the State or a political subdivision of the State. By submitting a bid, or entering into a contract with the State, Vendor is affirming that (1) for construction contracts, the Vendor is not in default on any monetary obligation owed to the state or a political subdivision of the state, and (2) for all other contracts, neither the Vendor nor any related party owe a debt as defined above, and neither the Vendor nor any related party are in employer default as defined in the statute cited above unless the debt or employer default is permitted under the statute.

38. CONFLICT OF INTEREST: Vendor, its officers or members or employees, shall not presently have or acquire an interest, direct or indirect, which would conflict with or compromise the performance of its obligations hereunder. Vendor shall periodically inquire of its officers, members and employees to ensure that a conflict of interest does not arise. Any conflict of interest discovered shall be promptly presented in detail to the Agency.

39. REPORTS: Vendor shall provide the Agency and/or the Purchasing Division with the following reports identified by a checked box below:

☑ Such reports as the Agency and/or the Purchasing Division may request. Requested reports may include, but are not limited to, quantities purchased, agencies utilizing the contract, total contract expenditures by agency, etc.

☐ Quarterly reports detailing the total quantity of purchases in units and dollars, along with a listing of purchases by agency. Quarterly reports should be delivered to the Purchasing Division via email at purchasing.division@wv.gov.

40. BACKGROUND CHECK: In accordance with W. Va. Code § 15-2D-3, the State reserves the right to prohibit a service provider's employees from accessing sensitive or critical information or to be present at the Capitol complex based upon results addressed from a criminal background check. Service providers should contact the West Virginia Division of Protective Services by phone at (304) 558-9911 for more information.

41. PREFERENCE FOR USE OF DOMESTIC STEEL PRODUCTS: Except when authorized by the Director of the Purchasing Division pursuant to W. Va. Code § 5A-3-56, no contractor may use or supply steel products for a State Contract Project other than those steel products made in the United States. A contractor who uses steel products in violation of this section may be subject to civil penalties pursuant to W. Va. Code § 5A-3-56. As used in this section:

a. "State Contract Project" means any erection or construction of, or any addition to, alteration of or other improvement to any building or structure, including, but not limited to, roads or highways, or the installation of any heating or cooling or ventilating plants or other equipment, or the supply of and materials for such projects, pursuant to a contract with the State of West Virginia for which bids were solicited on or after June 6, 2001.

b. "Steel Products" means products rolled, formed, shaped, drawn, extruded, forged, cast, fabricated or otherwise similarly processed, or processed by a combination of two or more or such operations, from steel made by the open heath, basic oxygen, electric furnace, Bessemer or other steel making process.

c. The Purchasing Division Director may, in writing, authorize the use of foreign steel products if:

    1. The cost for each contract item used does not exceed one tenth of one percent (.1%) of the total contract cost or two thousand five hundred dollars ($2,500.00), whichever is greater. For the purposes of this section, the cost is the value of the steel product as delivered to the project; or

    2. The Director of the Purchasing Division determines that specified steel materials are not produced in the United States in sufficient quantity or otherwise are not reasonably available to meet contract requirements.

42. PREFERENCE FOR USE OF DOMESTIC ALUMINUM, GLASS, AND STEEL: In Accordance with W. Va. Code § 5-19-1 et seq., and W. Va. CSR § 148-10-1 et seq., for every contract or subcontract, subject to the limitations contained herein, for the construction, reconstruction, alteration, repair, improvement or maintenance of public works or for the purchase of any item of machinery or equipment to be used at sites of public works, only domestic aluminum, glass or steel products shall be supplied unless the spending officer determines, in writing, after the receipt of offers or bids, (1) that the cost of domestic aluminum, glass or steel products is unreasonable or inconsistent with the public interest of the State of West Virginia, (2) that domestic aluminum, glass or steel products are not produced in sufficient quantities to meet the contract requirements, or (3) the available domestic aluminum, glass, or steel do not meet the contract specifications. This provision only applies to public works contracts awarded in an amount more than fifty thousand dollars ($50,000) or public works contracts that require more than ten thousand pounds of steel products.

The cost of domestic aluminum, glass, or steel products may be unreasonable if the cost is more than twenty percent (20%) of the bid or offered price for foreign made aluminum, glass, or steel products. If the domestic aluminum, glass or steel products to be supplied or produced in a "substantial labor surplus area", as defined by the United States Department of Labor, the cost of domestic aluminum, glass, or steel products may be unreasonable if the cost is more than thirty percent (30%) of the bid or offered price for foreign made aluminum, glass, or steel products. This preference shall be applied to an item of machinery or equipment, as indicated above, when the item is a single unit of equipment or machinery manufactured primarily of aluminum, glass or steel, is part of a public works contract and has the sole purpose or of being a permanent part of a single public works project. This provision does not apply to equipment or machinery purchased by a spending unit for use by that spending unit and not as part of a single public works project.

All bids and offers including domestic aluminum, glass or steel products that exceed bid or offer prices including foreign aluminum, glass or steel products after application of the preferences provided in this provision may be reduced to a price equal to or lower than the lowest bid or offer price for foreign aluminum, glass or steel products plus the applicable preference. If the reduced bid or offer prices are made in writing and supersede the prior bid or offer prices, all bids or offers, including the reduced bid or offer prices, will be reevaluated in accordance with this rule.

43. INTERESTED PARTY SUPPLEMENTAL DISCLOSURE: W. Va. Code § 6D-1-2 requires that for contracts with an actual or estimated value of at least $1 million, the Vendor must submit to the Agency a disclosure of interested parties prior to beginning work under this Contract. Additionally, the Vendor must submit a supplemental disclosure of interested parties reflecting any new or differing interested parties to the contract, which were not included in the original pre-work interested party disclosure, within 30 days following the completion or termination of the contract. A copy of that form is included with this solicitation or can be obtained from the WV Ethics Commission. This requirement does not apply to publicly traded companies listed on a national or international stock exchange. A more detailed definition of interested parties can be obtained from the form referenced above.

44. PROHIBITION AGAINST USED OR REFURBISHED: Unless expressly permitted in the solicitation published by the State, Vendor must provide new, unused commodities, and is prohibited from supplying used or refurbished commodities, in fulfilling its responsibilities under this Contract.

45. VOID CONTRACT CLAUSES: This Contract is subject to the provisions of West Virginia Code § 5A-3-62, which automatically voids certain contract clauses that violate State law.

46. ISRAEL BOYCOTT: Bidder understands and agrees that, pursuant to W. Va. Code § 5A-3-63, it is prohibited from engaging in a boycott of Israel during the term of this contract.

DESIGNATED CONTACT: Vendor appoints the individual identified in this Section as the Contract Administrator and the initial point of contact for matters relating to this Contract.

(Printed Name and Title) Hallie Morgan, VP Quality and Data Services

(Address) West Virginia Hospital Association 100 Association Drive Charleston WV 25311

(Phone Number) / (Fax Number) (304) 353-9714 / (304) 414-0210

(email address) hmorgan@wvha.org

CERTIFICATION AND SIGNATURE: By signing below, or submitting documentation through wvOASIS, I certify that: I have reviewed this Solicitation/Contract in its entirety; that I understand the requirements, terms and conditions, and other information contained herein; that this bid, offer or proposal constitutes an offer to the State that cannot be unilaterally withdrawn; that the product or service proposed meets the mandatory requirements contained in the Solicitation/Contract for that product or service, unless otherwise stated herein; that the Vendor accepts the terms and conditions contained in the Solicitation, unless otherwise stated herein; that I am submitting this bid, offer or proposal for review and consideration; that this bid or offer was made without prior understanding, agreement, or connection with any entity submitting a bid or offer for the same material, supplies, equipment or services; that this bid or offer is in all respects fair and without collusion or fraud; that this Contract is accepted or entered into without any prior understanding, agreement, or connection to any other entity that could be considered a violation of law; that I am authorized by the Vendor to execute and submit this bid, offer, or proposal, or any documents related thereto on Vendor's behalf; that I am authorized to bind the vendor in a contractual relationship; and that to the best of my knowledge, the vendor has properly registered with any State agency that may require registration.

By signing below, I further certify that I understand this Contract is subject to the provisions of West Virginia Code § 5A-3-62 which automatically voids certain contract clauses that violate State law; and that pursuant to W. Va. Code 5A-3-63, the entity entering into this contract is prohibited from engaging in a boycott against Israel.

WEST VIRGINIA HOSPITAL ASSOCIATION
(Company)

(Signature of Authorized Representative)

M. JAMES KAUFMAN PRESIDENT + CEO, 2/23/24
(Printed Name and Title of Authorized Representative) (Date)

304-353-9713 / FAX 304-414-0210
(Phone Number) (Fax Number)

JKAUFMAN@WVHA.ORG
(Email Address)

SPECIFICATIONS

1. **PURPOSE AND SCOPE:** The West Virginia Purchasing Division is soliciting bids on behalf of the Office of Shared Administration for the WV Health Care Authority (HCA) (when used in these documents the terms "Department" or "Agency" refer to HCA or state entities authorized to represent HCA) to upgrade or replace the existing Hospital Inpatient Data System (HIDS) with a system that will maintain and improve data collection for services rendered in both inpatient and non-inpatient settings including Emergency Departments, hospital based outpatient surgery; outpatient observation stays; outpatient diagnostic and therapeutic hospital services; and other types of hospital outpatient services by West Virginia hospitals and other relevant providers. The new or upgraded system will be referred to as the Hospital Universal Billing Data System (HUBDS).

   The vendor will collect, process and edit data on behalf of the Agency in accordance with West Virginia State Code §16-29B This article may be accessed at http://www.wvlegislature.gov/WVCODE/Code.cfm?chap=16&art=29B) and the Financial Disclosure Rule, 65 C.S.R. § 13 (The complete rule may be found at: http://apps.sos.wv.gov/adlaw/csr/) and applicable state laws and rules. This data will be used to satisfy certain public health reporting requirements and to inform the Department on regulatory and policy decisions and may be distributed to policy makers, providers, researchers, and consumers via standard reports; special data requests; participation in the Agency for Healthcare Research and Quality's (AHRQ's) Healthcare Cost and Utilization Project (HCUP); and other appropriate means.

   Vendor will offer a secure, web-based system for online submission and editing of data. Except where specifically noted in this RFQ, data collection, submission, edit checking and reporting will follow the guidelines, procedures and policies established by WV HCA for the HUBDS. Links to these materials on the HCA website are included in the RFQ Section 3.1.11 - Documentation.

   Current Operating Environment: HCA stores Hospital UB Data in a SQL database at the Office of Management Information Services within the Office of Shared Administration.

   NOTE: This request is covered in part or in whole by federal funds. All bidders will be required to acknowledge and adhere to Attachment A - "Federal Funds Addenum"

2. **DEFINITIONS:** The terms listed below shall have the meanings assigned to them below. Additional definitions can be found in section 2 of the General Terms and Conditions.

2.1 "Contract Item" or **"Contract Items"** means the list of items identified in Section 3.1 below and on the Pricing Pages.

2.2 "Pricing Pages" means the schedule of prices, estimated order quantity, and totals contained in wvOASIS or attached hereto as Exhibit A, and used to evaluate the Solicitation responses.

2.3 "ANSI ASC" means American National Standards Institute, Accredited Standards Committee.

2.4 "CDA®" means Clinical Document Architecture is a document markup standard that specifies the structure and semantics of "clinical documents" for the purpose of exchange between healthcare providers and patients.

2.5 "CMS" means Centers for Medicare and Medicaid Services.

2.6 "DHHR" means any reference to the former WV Department of Health and Human Resources.

2.7 "DO" means Delivery Order-may be referred to as "ADO" or "CDO"

2.8 "Downtime" means the time during which any component(s) of the solution is not functioning or available for any reason. Production downtime is the time during which the solution is not available for its intended use in production.

2.9 "DRG" means Diagnosis-related group.

2.10 "HCA" means the WV Healthcare Authority, under the WV Department of Health.

2.11 "HIDS" means the Hospital Inpatient Data System which is the system to be upgraded or replaced through this solicitation.

2.12 "HL7 or HL7 v2. X and v3.x" means Health Level 7 International, version.

2.13 "ICD-9-CM or ICD-10 CM" means International Classification of Diseases, Ninth Revision, Clinical Modification and International Classification of Diseases, Tenth Revision, Clinical Modification.

2.14 "NIST" means National Institute of Standards and Technology

2.15 "Not Applicable" is when used in the context of the Procurement Library Source field and in the requirements tables contained in this appendix, Not Applicable indicates that the requirements were sourced directly from State subject matter experts during Joint Requirements Planning sessions or identified through some other means that did not allow the State to reference a specific source document.

2.16 "Notice" refers to usage of this term refers to the Notice of Decision. The Notice is the prescribed printed communication from the office to the client. Notices are typically generated for both evaluated and determined Assistance Groups (AGs).

2.17 "Notification" means a system-generated notice that is sent to a client or applicant either through mail or email to notify of any pending or potential actions to be taken on the case.

2.18 "PDF" means Portable Document Format

2.19 "RFQ" means Request for Quotation.

2.20 "SAS" means Statistical Analysis System

2.21 "Scheduled Downtime" means any period the solution, or any component(s) of the solution, is unavailable for its intended use. Scheduled downtime should be reviewed and approved by the State in advance of the service interruption. Scheduled downtime, that has received approval from the Department, does not count towards downtime performance standards.

2.22 "SLA" means Service Level Agreement (s)

2.23 "SME" means Subject Matter Expert

2.24 "Solicitation" means the official notice of an opportunity to supply the State with goods or services that is published by the Purchasing Division.

2.25 "SOW" means Statement of Work

2.26 "System" means the data system proposed by the vendor to upgrade or replace HIDS.

2.27 "System Maintenance" means the time available to the Vendor to perform hardware and software maintenance.

2.28 "Unscheduled Downtime" means any period the solution, or any component(s) of the solution, is unavailable for its intended use wherein the Department has not approved the downtime in advance of the service interruption. Unscheduled downtime should be reported to the Department within one (1) hour of occurrence.

2.29 "Vendor" means the entity providing the services defined in this RFQ to the State. Synonyms: the contractor, service provider

2.30 "WVOT" means the West Virginia Office of Technology.

2.31 "XLS or XLSX" means an Excel Sheets binary file format which holds information about the worksheets in a file, including both content and formatting, the standard extension for the modern Microsoft Excel spreadsheet files.

3. GENERAL REQUIREMENTS:

3.1 Contract Items and Mandatory Requirements: Vendor shall provide Agency with the Contract Items listed below on an open-end and continuing basis. Contract Items must meet or exceed the mandatory requirements as shown below.

IMPORTANT INFORMATION – This solicitation is a request for quotation (RFQ) and the award will be to the lowest responsive bidder. By submitting a bid, the Vendor certifies that they will meet each of the RFQ requirements, including requirements for the Optional Module (see 3.1.3.2.11) and Optional Services (see 3.1.8.1), if ordered by the Agency during the life of the contract.

3.1.1 Qualifications: Vendor, or vendor's staff if requirements are inherently limited to individuals rather than corporate entities, shall have the following minimum qualifications:

3.1.2 Qualifications and Experience:

3.1.2.1 Vendor **MUST** have a minimum of 10 years of experience collecting Hospital Billing data in a then current standard format such as ANSI (American National Standards Institute, Accredited Standards Committee). ASC X12 8371 4010.

3.1.2.2 Vendor **MUST** have verifiable experience exchanging clinical data in HL7 (American National Standards Institute, Accredited Standards Committee). v2.x and v3.x

and experience collecting, editing and using data coded, ICD-10-CM.

3.1.2.3 Vendor **MUST** have a minimum of 10 years of experience operating a secure web-based system for standards based on-line data submission.

3.1.2.4 Within 10 working days of contract award the vendor **MUST** provide the Agency with a representative staffing plan that covers, at a minimum, a project manager, a functional/operational lead, a programmer, a trainer, and a data analyst. A single staff member may fill multiple roles but must satisfy the qualifications for each role. Provide resumes, including degrees and certificates applicable to this project for proposed staff. If you are proposing the same staff member to fill multiple roles include an estimate of the percentage of time the member will spend in each role. Resumes must demonstrate at least:

3.1.2.4.1 **PROJECT MANAGER** – Minimum of 5 years of experience managing projects similar in size and scope to this project.

3.1.2.4.2 **FUNCTIONAL/OPERATIONAL LEAD** – Minimum of 3 years of experience in a lead role on projects similar in scope and size to this project including experience trouble-shooting NW/Communications problems from submitters to the on-line system.

3.1.2.4.3 **PROGRAMMER** – Minimum of 3 years of experience programming with modern programming languages and interacting with data stored in Oracle and SQL Server databases.

3.1.2.4.4 **TRAINER** – Minimum of 2 years of experience training end users on the use of the proposed on-line data submission tool.

3.1.2.4.5 **DATA ANALYST** – Minimum of 2 years of experience analyzing data and producing reports utilizing data analytics tools such as IBM Cognos, Microsoft Power BI, or other commercially available data analytics tools.

3.1.2.5 Over the life of the contract, Vendor may substitute other staff for those named in 3.1.2.4.1 as long as the substitute meets the minimum requirements listed therein.

3.1.2.6 If any portions of the program will be subcontracted, vendor **MUST** identify in the bid those subcontractors that it intends to use and the portions of the program to be assigned to each. Vendor must notify the Agency 15 days in advance. If no subcontractor is identified in the submitted bid subcontracting will not be permitted.

3.1.2.7 Documentation will be required prior to a contract award and may be in any form the State requires - references, past project documentation, etc.

3.1.3 Mandatory Requirements

3.1.3.1 **Mandatory Contract Services Requirements and Deliverables:** Contract Services must meet or exceed the mandatory requirements listed below.
Contract Items and Mandatory Requirements: Vendor shall provide Agency with the Contract Items listed below on an open-end and continuing basis. Contract Items must meet or exceed the mandatory requirements as shown below Contract Services must meet or exceed the mandatory requirements listed below.

3.1.3.2 **Data Collection Processing and Editing**

3.1.3.2.1 HOSPITAL UB DATA: Vendor **SHALL** collect, process, maintain, and assure the quality of hospital discharge electronic billing data including Inpatient, Emergency Department, Outpatient Surgery, Outpatient Observation Stays, Outpatient Diagnostic and Therapeutic Hospital Services from all 63 non-federal hospitals in West Virginia in accordance with the West Virginia Hospital Data Submission System, Data Collection Policies and Procedures (See Section 3.1.11).

3.1.3.2.2 Vendor **SHALL** collect the hospital uniform billing (UB) data elements outlined in the *Data Element Specifications Guide* (See Section 3.1.11) and implement annual additions and/or modifications to reported data elements based on changes in state, federal, or industry standards or policies, including but not limited to ICD-10-CM, in a manner and timeline approved by the Health Care Authority.

3.1.3.2.2.1 Vendor **SHALL** agree to process in accordance to federal regulations or guidance the collection of expected sources of payment, revising the payer codes and updating user documentation. Source of payment is currently reported in accordance with the *West Virginia Hospital Inpatient Data System Payer Coding Specifications* (See Section 3.1.11).

3.1.3.2.2.2 Vendor **SHALL** accept hospital data files in the current West Virginia UB-04 Extended Data Layout (See Section 3.1.11) and ANSI ASC X12 837i 5010 https://www.cms.gov/Medicare/Billing/ElectronicBillingEDITrans/downloads/5010A2837ACG.pdf (See Section 1) formats that accommodate the data elements outlined in 3.1.3.2.2

3.1.3.2.2.3 Vendor **SHALL** assess and confirm the accuracy, completeness, quality, appropriateness, and reasonability of the submitted data to identify and eliminate common errors. Implement current edit checks, as outlined in the *Edit Check Definitions* guide (See Section 3.1.11). Identify data submission and processing errors. Implement additional or revised edits over the course of the contract based upon identified data quality issues; revised reporting requirements; or changes to coding, billing, and reimbursement

standards, as requested, required, and/or approved by the agency.

3.1.3.2.3 Vendor **SHALL** continually evaluate the data collection, processing, and editing procedures for performance and compliance; routinely implement quality improvements, based on these reviews, to enhance system processes, efficiencies, and speed, as requested and/or approved by the HCA.

3.1.3.2.4 Beginning 30 days prior to each quarterly submission deadline, vendor **SHALL** submit a report twice weekly (on Tuesday and Friday, unless either of those days fall on a Federal Holiday in which case no report is due until the next Tuesday or Friday) showing which hospitals have submitted a final data report for the quarter. Reports should be submitted electronically to HCA and the Office of Shared Services. Reporting contacts and email addresses will be provided within 30 days of contract award.

3.1.3.2.5 Vendor **MUST** maintain a secure web-based system for the online submission and editing of hospital UB data and implement updates or revisions to the system based on changes adopted per 3.1.3.2.1, 3.1.3.2.2, and 3.1.3.2.3 above.

3.1.3.2.6 Vendor **SHALL** maintain a master database of all data collected during the contract period and develop and implement processes that allow for an audit trail of all submissions, additions, changes, and deletions to the master database.

3.1.3.2.7 Vendor **SHALL** implement methods to link all records submitted for a single discharge (including interim, replacement, and late charges bills) and create and/or identify a single complete (analytic) record representing each encounter, based on HCA adjudication requirements, generally accepted industry standards, and record characteristics, such as patient control number, bill type, and discharge date.

3.1.3.2.8 Vendor **SHALL** develop and make available to data submitters and the Agency, reports that promote the assessment of the quality and completeness of data submitted to the master database. The data quality reports should be updated on a reasonable and routine basis to summarize recently submitted data and be available in common formats (e.g., PDF, Excel, etc.).

3.1.3.2.9 Vendor **SHALL** provide a web-based, user self-service reporting tool for 200 submitters and Agency Staff to perform data analytics and produce simple ad hoc reports.

3.1.3.2.9.1 The self-service reporting tool **MUST** restrict submitter access to only the data they have submitted.

3.1.3.2.9.2 The self-service reporting tool **MUST** allow users to store an unlimited number of queries and standard reports.

3.1.3.2.10 Vendor **SHALL** provide resources or tools to assist the HCA (Health Care Authority) with the quarterly reconciliation of the master database. Currently, hospitals submit to the HCA a quarterly reconciliation report summarizing the number of discharges by provider number (CMS Certification Number), month, and HCA payer classification (available for download on the HCA website). This report is manually compared to a report of the data contained in the master database. Hospitals are notified by the HCA of discrepancies and must revise the submitted data, as requested by the HCA.

3.1.3.2.11 ADDITIONAL OPTIONAL SYSTEM MODULE: Vendor **MUST** propose a system that may expand (at the option of the Agency) to accept and report Hospital Readmission Data.

Overview: Hospital readmissions occur when patients are readmitted to a hospital within 30 days after being discharged from an earlier hospital stay. Hospitals are encouraged to reduce readmissions by

the Center for Medicare and Medicaid Services (CMS) who penalize excess readmissions for select conditions as part of Readmissions Reduction Program. Hospitals with excessive readmissions receive lower payments when reimbursed through the Inpatient Prospective Payment System. The ability to provide readmission statistics to the WV DoH and WV Hospitals will facilitate the improvement of care and process improvements and will translate to cost savings for WV Payers.

Technical Summary: Upon WV DoH's approval to develop the optional module, the selected vendor will develop, validate and implement a method to track all patients and readmissions between hospitals and provide a report summarizing the methodology and findings on a quarterly basis. The most current 3 years of patient level data submitted by hospitals as a part of the UB Discharge Data submissions program will be used to develop a master patient index (MPI). Data fields utilized may include (but are not limited to) date of birth, patient full name, sex, Social Security Number, and address. Once the MPI is developed, readmission reports may be created and made available. This process will be repeated every quarter to provide the WV DoH with readmission findings and analyses. The methodology will utilize the comorbidities that CMS uses for risk adjustment and apply the same algorithm for assigning unplanned/planned readmissions as CMS. The data will include all patients 18 years and older and will include all payers. Additional technical information may be found in the Novetta HIDI Overview which can be found in Section 3.1.11 of this RFQ. This Optional System Module will be priced separately as a firm, fixed cost per calendar quarter for each quarter after the WV DoH authorizes implementation of the optional module.

3.1.4 Documentation and Technical Support

3.1.4.1 Vendor **SHALL** develop and provide documentation, training, and technical support regarding data collection, editing, and reconciliation for the mandatory system elements beginning upon contract award and for optional modules if and when implemented.

3.1.4.1.1 Vendor **SHALL** develop materials similar in content to the documents referenced in Section 1 of this RFQ. Provide the materials to WV DoH in a format suitable for inclusion on the HCA or other web sites. Maintain and update the files as necessary or as requested by DoH over the life of the contract. DoH will request revisions 30 days prior.

3.1.4.1.2 Within 30 working days, Vendor **SHALL** provide documentation to the Agency that details the operational processes of the web-based data submission system necessary for HCA staff to evaluate effectiveness and understand and communicate information about the system to data submitters. Acceptable format; word and Adobe PDF.

3.1.4.1.3 Vendor **SHALL** provide training and technical support to the Agency, data submitters, and/or their representatives on topics related to file formats, data submission, editing, and coding and billing standards.

3.1.4.1.3.1 Within 15 working days of the contract award, vendor **SHALL** provide Agency staff with at least one on-site, hands-on training and provide user documentation and access to online resources such as help files and training videos that can be linked to on the HCA or other WV agency web sites.

3.1.4.1.3.2 Within 15 working days of the contract award date vendor **SHALL** provide at least one live webinar for 70 data submitters and their representatives on topics related to file formats, data submission, editing, and coding and billing standards. Provide links

that can be placed on the HCA or other Agency web site to a video of the webinar or other training video that presents essentially the same material. Provide links to any other submitter specific documentation that is referenced in the training. A pre-recorded webinar must be available.

3.1.4.1.4 Vendor **SHALL** make all training materials, including videos available to help desk staff to utilize in responding to user requests.

3.1.5 Analytic Files

3.1.5.1 Vendor **SHALL** create and provide to the Agency weekly adjudicated analytic files containing submitted fields, appropriate groupers and adjustment factors, and other demographic, cost, clinical, and quality fields.

3.1.5.1.1 Vendor **SHALL** create and provide to the Agency, data file(s) containing all of the records and data elements submitted by hospitals, adjudicated records flagged for analysis, and processing and analytic fields created by the Vendor (including MDC, DRG, and other useful indicators of services, payment, cost, severity of illness, risk of mortality, intensity of service, and quality of care that will enhance the Agency analysis). The minimum fields required in the analytic files are outlined in Attachment B.

3.1.5.1.2 Vendor **SHALL** deliver the file(s) to the Agency in a secure electronic format .PDF,.TXT or others as approved by the Agency and acceptable for import into the Agency's then current operating environment. (SEE CURRENT OPERATING ENVIRONMENT IN section 1 of this RFQ)

3.1.5.1.3 Vendor **MUST** maintain and provide to the HCA documentation, reference files, and data dictionaries detailing the contents of the data file(s) and any information necessary or useful for HCA in its review and analysis of the data, including but not limited to: a data element frequency report; file layouts; load programs; code value definitions and

labels; custom programming code; and descriptions of the methodologies related to the creation of the calculated fields added to the file(s) by the Vendor.

3.1.5.1.4 Vendor **SHALL** create and provide to the HCA, on a routine basis, new reports (current standard reports are described in the UB data request form available for download on the HCA website) from the analytic file(s) that summarize key utilization, access, cost, and quality indicators, such as: patient days; case-mix; market share and service areas; and common DRGs/diagnoses/procedures by patient demographic characteristics, geographic region, and/or hospital. Propose a series of reports to be developed during the first project year. In subsequent project years, plan for three modifications to current reports and for the development of two new reports annually.

3.1.6 Data Security and Privacy

3.1.6.1 Vendor **MUST** implement administrative, physical, and technical safeguards to ensure the confidentiality, integrity and availability of all System data the Vendor creates, receives, maintains, or transmits, in accordance with federal and state laws and regulations (including the HIPAA Security Rule, 45 CFR § 164.302), this contract, and Agency policies.

3.1.6.1.1 Within 30 working days, Vendor **MUST** comply with all HIPAA Security administrative safeguards, Including:

3.1.6.1.1.1 Undertake a valid risk assessment and establish an effective risk management program for the System.

3.1.6.1.1.2 Within 30 working days, implement procedures to regularly review records of information systems activity, such as audit logs, access reports, and security incident tracking reports.

3.1.6.1.1.3 Conduct security audits, at the request of HCA or WVOT, to evaluate the appropriateness and effectiveness of policies

and procedures for protection of privacy, confidentiality, and security of the System data, including an analysis of the mechanisms used for data transfer and storage. The audit may include a review of the networking and computer facilities used by the System, penetration testing, or an active assault on the preliminary evaluation of basic data security issues; therefore, some sources of risk may only need to be evaluated categorically (i.e., significant vs. not significant). The frequency of reviews and updates is "within 365 days". The audit should be conducted by an external subcontractor with expertise in the field of data security. A report on the results of the security audit should contain at a minimum: effectiveness/ineffectiveness of current data security policy and procedures, including receipt of data, storage, handling printouts, LAN access, remote access, staff knowledge and compliance, data transmission, and loss control security risks not addressed in the report. If appropriate, the report should address how findings compared to standards relevant to general businesses that develop research files for the government. If significant data security risks are identified by the audit, the report should recommend measures by which such risks can be minimized. Additional audits may be required to assess new threats or to evaluate the effectiveness of remediation steps taken to resolve problems.

3.1.6.1.1.4 Have security policies and procedures in place for Vendor staff, which include appropriate sanctions for staff that act contrary to such policies and procedures. Implement a security awareness and training program for all members of the vendor workforce. The State may require that a vendor provide evidence of adequate background checks, including a nationwide

record search, for individuals who are entrusted by the vendor to work with State information. Significant and substantive changes need to be submitted as far in advance as reasonably possible for the Agency consideration. It is possible that the Agency may have to forward any proposed changes to our federal regulators for review and authorization at least 45-days in advance of implementation to production environments. The Agency will have to follow appropriate reporting methods for each federal agency as appropriate. Typical project status updates and reports take place weekly under normal circumstances. In times of urgency or emergency, reporting would take place immediately, but not to exceed one hour.

3.1.6.1.1.5 Establish emergency/backup/disaster plans and contingencies for the System. Within 30 days of contract award, the Agency should receive copies and reserve the right to request changes.

3.1.6.2 Vendor **MUST** comply with all HIPAA Security physical safeguards, including the establishment of adequate Vendor facility access controls and device and media controls.

3.1.6.3 Vendor **MUST** comply with all HIPAA Security technical safeguards, including:

3.1.6.3.1 Secure and appropriate authentication of all users of the data immediately, but no longer than one hour, upon initial receipt of request.

3.1.6.3.2 Support role-based access to data.

3.1.6.3.3 Incorporate and employ an effective and efficient audit mechanism for tracking access to System data, including the preparation, update, and maintenance of audit logs.

3.1.6.3.4 Provide for automatic notification of certain non-routine or unscheduled access of System data to designated personnel, as appropriate.

3.1.6.3.5 Provide for automatic notification of certain non-routine or unscheduled access of System data to designated personnel, as appropriate.

3.1.6.3.6 Employ systemic mechanisms, including anti-virus and intrusion detection software, to ensure the integrity of data from improper alteration and destruction, and to corroborate the data's ongoing integrity, in compliance with HIPAA.

3.1.6.4 Vendor **SHALL** ensure that data maintained on behalf of the System is not used, released, or sold without the specific authorization of the Agency, regardless of whether the data has been de-identified or included within a limited data set

3.1.6.5 Vendor **SHALL** implement appropriate notification procedures upon the discovery or suspicion of a breach of security of System data.

3.1.6.6 Vendor **SHALL** review and revise policies and procedures to ensure data security and privacy are in accordance with the current federal and state laws, and Agency standards and policies.

3.1.6.7 The vendor **SHALL** certify that it is not currently under investigation by any state or federal authority for a breach of data security.

3.1.6.8 The vendor **MUST** disclose whether it has been involved in any breach of data security and provide details relating to the causes of the breach, the mitigating actions taken in response to the breach, and whether notification of affected consumers was undertaken.

3.1.6.9 The vendor **MUST** disclose details of any previous investigations by any state or federal authority related to privacy or security of patient information. The details must include the resulting corrective action plan or details of the final resolution, including the assessment of any fines or other sanctions against the vendor.

3.1.6.10 The vendor **MUST** certify that it has never been convicted of, charged with, or is under investigation for, violation of any

criminal law, or violation of any civil law governing health care fraud, abuse, or waste.

3.1.6.11 The vendor **MUST** Certify that it does not employ any individuals who have been excluded or debarred by the federal or any state government from participating in any federal or state program or contract.

3.1.7 Project Management

3.1.7.1 Vendor **MUST** provide project management, consulting, analysis, and reporting services to ensure successful project implementation.

3.1.7.1.1 Vendor **SHALL** communicate project status not less frequently than monthly with the Agency regarding project status, including data submission activities, potential problems or barriers to project implementation, and contacts/communications with data submitters.

3.1.7.1.2 Upon request, Vendor **SHALL** provide consultation and recommendations to the Agency regarding data analysis, reporting, and dissemination activities aimed at assessing the utilization, access, cost, and quality of healthcare.

3.1.7.1.3 Within 30 working days, Vendor **SHALL** create systems, programs, and processes that are flexible enough to integrate updates and revisions in a timely manner, as required and/or requested by the Agency, without creating undue burden on resources.

3.1.7.1.4 Vendor **SHALL** respond to Agency inquiries or requests for technical assistance and/or project revisions/updates within two (2) business days, based on the urgency and importance of the issue as determined by the Agency.

3.1.7.1.5 Vendor **SHALL** acquire or provide any necessary hardware, software, and reference data files to complete all tasks the Vendor proposes to perform in fulfillment of the project specifications and to meet all applicable timeframes set forth in this

RFQ. Data obtained for the sole purpose of the performance of this contract must not be used for any other purpose outside of the Agency contract.

3.1.7.1.6 Vendor **SHALL** cover all costs associated with providing technical assistance, training, and status reports to Agency and data submitters, including teleconferencing, webinars, and/or travel to a minimum of two onsite meetings each year.

3.1.8 Optional Services

3.1.8.1 The Vendor **MUST** include pricing for the optional services listed in 3.1.8.1.1 through 3.1.8.1.7 Pricing for optional services **MUST** be an hourly rate and **MUST** be separate from pricing for the Mandatory services enumerated in sections 3.1.3.2.1 through 3.1.3.2.11. The decision to utilize the optional services at any time during the contract is entirely at the discretion of the Agency. The Agency will request a Statement of Work (SOW) from the vendor for any optional services desired. The SOW MUST include a detailed breakdown of the hours required to complete the request. The SOW represents a not to exceed estimate. If the SOW is accepted by the Agency the work will be authorized through the Deliver Order (DO) process. No work may be billed for in the absence of a valid DO.

Vendor **MUST** provide an hourly rate for the services in 3.1.8.1.1 through 3.1.8.1.7. The Agency will request a statement of work (SOW) detailing the hours required for execution of the request for any optional services desired. The SOW represents a not to exceed price. Upon completion of the requested work, vendor will bill for hours actually worked up to the maximum number of hours included in the SOW.

3.1.8.1.1 Develop and deliver to AHRQ's Healthcare Cost and Utilization Project (HCUP) an annual adjudicated file, in a timeline and format required by the Agency.

3.1.8.1.2 Prepare and provide to the Agency the annual standard aggregated public use data files and standard reports, as described on the UB data

request form (See HCA Data Request Procedures and Forms in Section 3.1.11) to be disseminated by the Agency to data requesters.

3.1.8.1.3 Fulfill customer requests for subsets of adjudicated inpatient data, as approved and requested by the Agency, in accordance with then current Agency policies and procedures (See Section 1 for the current data disclosure policy).

3.1.8.1.4 Fulfill ad hoc analysis requests to answer occasional and special research questions of the Agency.

3.1.8.1.5 Develop and provide to the Agency an analysis of the risk of re identification of patients in the database based on the information contained in the final annual file in combination with other readily accessible data sources; recommend appropriate statistical disclosure limitation methods to increase patient confidentiality; and develop a limited data set, based on these recommendations, for release to requestors.

3.1.8.1.6 Provide tools, products, report templates, software, and/or code for use by the agency and/or external partners to conduct analysis of health care utilization, access, costs, and quality.

3.1.8.1.7 Develop and implement new data submission system enhancements, data quality reports, or analytic reports, determined necessary to perform the functions of this project but not elsewhere specified or required by this RFQ.

3.1.9 Data Ownership and Usage

3.1.9.1 The Vendor **AGREES** that all data and any software, programming code (including code to implement editing and adjudication procedures and to create non-proprietary analytic fields), file formats, or other deliverables developed to fulfill contract requirements, be the sole property of the Agency.

3.1.9.2 The Vendor **AGREES** that all data related to the execution of the contract is collected on behalf of, and remains the property

of, the Agency. Any other uses by the Vendor are subject to data use agreements which will be granted consistent with the Department's existing data use policies.

3.1.9.3 The Vendor **AGREES** to provide privacy and security safeguards to protect all data from any use or disclosure for any purpose other than that described within this solicitation or expressly authorized by the HCA Project Manager through written signed consent.

3.1.10 Milestones, Deliverables, and Service Level Agreements

3.1.10.1 The secure website **MUST** be available to data submitters and the Agency staff within 15 working days of the contract award.

3.1.10.1.1 Regardless of the dates of contract award and go live dates for the web-based data submission system, the vendor **AGREES** to include data from submitters back to 3/31/2024.

3.1.10.2 Live help desk support including telephone and on-line chat **SHALL** be available to data submitters, their representatives, and Agency Staff a minimum of 8 hours per day, Monday thru Friday during daytime business hours (EST), not including federal holidays, commencing on the first day the secure website is made available.

3.1.10.3 The Vendor **SHALL** conduct analyses to investigate and determine potential data quality issues, as requested by the HCA, within at least 10 working days of request.

3.1.10.3.1 The Vendor **MUST** correct identified data submission errors that are determined cannot or should not be corrected by the data submitter, as requested and/or approved by the Agency, within at least 20 working days of request/approval.

3.1.10.3.2 The Vendor **MUST** correct any identified errors in the System or the resulting file(s), which are attributable to the Vendor, within at least 10 working days of request.

3.1.10.3.3 The Vendor **SHALL** certify that the disaster recovery plan, as approved by the Agency, has been tested and proven effective within 60 working days of contract award.

3.1.10.3.4 The Vendor **MUST** deliver a final complete data file, for the previous calendar year, with all identified data quality issues resolved, by June 1 each year.

3.1.10.3.5 The Vendor **SHALL**, within 30 working days of the end of each contract year, provide to the HCA an annual report of the project, including but not limited to: project successes and barriers; revisions or updates implemented to the System during the project year; and any recommendations for future project and System enhancements.

3.1.10.3.6 The Vendor **SHALL**, at least 90 working days prior to each contract year, submit to HCA a final and approved annual detailed work plan of key activities and projects to be completed during the next contract year. The work plan must include an implementation timeline for key project activities and identify responsible team members.

3.1.10.3.7 The Vendor **SHALL** cooperate with the Agency and any subsequent Vendor should the contract, which is the subject of this RFQ, be terminated, and to deliver any and all data, documentation, and associated work products to the Agency or its designee within thirty (30) working days of receipt of notice of contract termination.

3.1.10.3.8 The Vendor **SHALL** destroy all data in the System at the end of the contract and/or upon the request of the Agency in accordance with NIST Special Publication 800-88 or the most current revision of that publication. Destruction of data **SHALL NOT** begin prior to receipt of written authorization from the Agency Project Manager and **SHALL** be completed within 30 days of receipt of that authorization.

3.1.10.3.9 If a Data breach is discovered or suspected Vendor **SHALL** immediately make the following notifications:

Agency Project Manager via email to:
dhhrmispurchasing@wv.gov

WV Office of Technology Service Desk by phone 304-558-9966

Agency Security Team via email to:
DHHRIncident@wv.gov

Notification is **REQUIRED** upon the **discovery** of breach of security of System data, where the use or disclosure is not provided for by this RFQ or contract, of which it becomes aware, if the System data was, or is reasonably believed to have been, acquired by an unauthorized person. If there is a **suspected** security incident, intrusion or unauthorized use or disclosure of PHI in violation of this RFQ or contract, or potential loss of System data affecting this RFQ or contract, then notification must occur within 24 hours by the same methods above. The Vendor shall immediately investigate such security incident, breach, or unauthorized use or disclosure of System data. Within 72 hours of the discovery, the Vendor shall notify the HCA Project Manager of: (a) What data elements were involved and the extent of the data involved in the breach; (b) A description of the unauthorized persons known or reasonably believed to have improperly used or disclosed System data; (c) A description of where the System data is believed to have been improperly transmitted, sent, or utilized; (d) A description of the probable causes of the improper use or disclosure; and (e) Whether any federal or state laws requiring individual notifications of breaches are triggered. The Agency will coordinate with the Vendor to determine additional specific actions that will be required of the Vendor for mitigation of the breach, which may include notification to the individual or other authorities. All associated costs shall be borne by the Vendor. This may include, but

not be limited to costs associated with notifying affected individuals.

3.1.11 Documentation: Links to procedural and technical documents referenced throughout the RFQ are provided below. Documentation available on the HCA website may reference the current system vendor, The West Virginia Hospital Association (WVHA). WVHA has assembled the documentation on behalf of HCA but does not own the standards and specifications referenced in the documents.

HCA Home: www.hca.wv.gov

Hospital Inpatient Data System:

https://hca.wv.gov/fdhome/HospInpatientData/Pages/default.aspx

West Virginia Hospital Data Submission System, Data Collection Policies and Procedures:

https://hca.wv.gov/fdhome/HospInpatientData/Documents/WVHIDS_PoliciesProcedures.pdf

West Virginia Hospital Data Submission System, Data Element Specifications Guide:
https://hca.wv.gov/fdhome/HospInpatientData/Documents/WVHDSS_DataElementSpecification.pdf

West Virginia Hospital Data Submission Systems, Edit Check Definitions, List of Warnings and Errors:
https://hca.wv.gov/fdhome/HospInpatientData/Documents/WVHDSS_EditChecks.pdf

Hospital Inpatient Data System Payer Coding Specifications:

https://hca.wv.gov/fdhome/HospInpatientData/Documents/WVHIDS_PayerCodes.pdf

West Virginia UB-04 Extended Data Layout: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/
https://hca.wv.gov/fdhome/HospInpatientData/Documents/WVHCA_UB04ExtLayout.pdf

West Virginia Hospital Data Submissions System, Data Collection Policies and Procedures:

https://hca.wv.gov/fdhome/HospInpatientData/Documents/WVHIDS_PoliciesProcedures.pdf

West Virginia Hospital Data Submission System, Payer Coding Specification:

https://hca.wv.gov/fdhome/HospInpatientData/Documents/WVHIDS_PayerCodes.pdf

HIPAA Security Rule (Includes 45 CFR 164.302)

https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/securityrulepdf.pdf?language=es

West Virginia, Office of Shared Administration, Office of Management Information Services policies:

http://www.wvdhhr.org/mis/policies.asp

Attachment C: WV Executive Branch Procedure: Response to Unauthorized disclosures.

Attachment D - WV Healthcare Authority Information Security and Privacy Policy

Attachment E - WVHCA Adjudication requirements

Attachment F- Policies Superseded by the Revised Information Security and Privacy Policy

Attachment G - Hospital Data Submission System User Guide

Attachment H - Novetta HIDI Overview

Attachment I – Hospital Data Submission System Data Collection Policies and Procedures

4. CONTRACT AWARD:

4.1 Contract Award: The Contract is intended to provide Agencies with a purchase price on all Contract Items. The Contract shall be awarded to the Vendor that provides the Contract Items meeting the required specifications for the lowest overall total cost as shown on the Pricing Pages.

4.2 Pricing Pages: Vendors must complete the pricing page (Excel Worksheet) that is included in this RFQ as Exhibit A. The pricing page must be completed in its entirety and returned/uploaded with the bid. There are three cost categories in this solicitation:

Base System Pricing which will be a firm fixed price for the Software and Services included in the base system. Base System Pricing is invoiced quarterly – the total cost for 3 months of software and services should be entered in Column B, Row 15. The spreadsheet should calculate the annual cost which will appear in Column D, Row 15. (If the cost does not calculate correctly, check the formula in Column D, it should be =B15*C15, if not, replace it with that formula).

Optional System Module (Hospital Readmission Data as described at 3.1.3.2.11) will also be a firm fixed price per calendar quarter. Optional System Module pricing is also invoiced quarterly once it is requested by the agency. Quarterly pricing goes in Column B, Row 17 and the formula in the worksheet will calculate the annual price which will be used for the cost evaluation. NOTE: The Agency may or may not authorize implementation of the Optional Module. If the Module is authorized it may not be authorized at the beginning of a contract quarter. If the agency requests and the vendor delivers the optional system module other than on the first day of a contract quarter, the first quarter's invoice shall be prorated based on the number of days it is available to the Agency in that quarter. (EXAMPLE: The module is delivered on the first day of May. 30 days of the quarter have already passed, the system is available for 61 calendar days. The invoice for the partial quarter would be the Quarterly Price multiplied by (61/91).

Optional Services are services that the Agency may request the vendor to perform on the State's behalf. These services are described in 3.1.8. Pricing for optional services is an hourly rate. Vendor must bid a single hourly rate that will apply to each of the optional services. The hourly rate is entered into Column B, Row 19. For evaluation purposes only, the pricing worksheet assumes 500 hours of optional service are requested each contract year and the total is calculated and added to Column D, Row 18.

Estimated first year costs are summed by the worksheet in Column D, Row 20.

Pricing must be included for each of the three Optional Renewal Years. Renewal year pricing does not need to be the same as the initial year pricing. PLEASE NOTE: You must enter a cost in Column B for each category in each Optional Renewal Year even if that cost is 0.00. Leaving any of the blue shaded cells blank will result in disqualification of the vendor's bid.

Contract award will be based on the Total for Entire Contract cost that appears in Column D, Row 46 of the Cost Sheet.

The Pricing Pages contain a list of the Contract Items and estimated purchase volume. The estimated purchase volume for each item represents the

approximate volume of anticipated purchases only. No future use of the Contract or any individual item is guaranteed or implied.

Vendor should electronically enter the information into the Pricing Pages through wvOASIS, if available, or as an electronic document

5. ORDERING AND PAYMENT:

5.1 Ordering: Vendor shall accept orders through wvOASIS, regular mail, facsimile, e-mail, or any other written form of communication. Vendor may, but is not required to, accept on-line orders through a secure internet ordering portal/website. If Vendor has the ability to accept on-line orders, it should include in its response a brief description of how Agencies may utilize the on-line ordering system. Vendor shall ensure that its on-line ordering system is properly secured prior to processing Agency orders on-line.

5.2 Payment: Agency shall pay the quarterly rate for the base system and/or optional modules and the hourly rate for optional services (billed quarterly), as shown on the Pricing Pages, for all Contract Services performed and accepted under this Contract. Vendor shall accept payment in accordance with the payment procedures of the State of West Virginia.

5.2.1 Invoices

5.2.1.1 Vendor **SHALL** submit quarterly invoices at the close of each calendar quarter for the hospital UB data systems and for any optional system modules ordered by WV Department of Health in that calendar quarter.

5.2.1.1.1 The first quarterly billing shall be prorated based on the contract award date.

5.2.1.2 For any optional services (See RFQ Section 3.1.8) ordered on a Delivery Order (DO) by the Agency the vendor **MAY** submit monthly invoices one month in arrears. Invoices will be for actual hours worked not to exceed the maximum number of hours authorized on the Delivery Order.

5.2.1.3 Invoices for the HUBDS and for any optional system modules ordered and authorized by the Agency will be reviewed by the Agency and paid in full if it is determined that all of the services, milestones, deliverables, and service level agreements for quarter have been met. If the Agency determines that there are significant unmet milestones, deliverables or service levels

for the quarter, the Agency will notify the vendor and may withhold payment of up to 15% of the invoice amount for each unmet item. Vendor **MAY** submit new invoices for withheld payments upon completion of the work.

6. **PERFORMANCE:** Vendor and Agency shall agree upon a schedule for performance of Contract Services and Contract Services Deliverables, unless such a schedule is already included herein by Agency. In the event that this Contract is designated as an open-end contract, Vendor shall perform in accordance with the release orders that may be issued against this Contract.

7. **DELIVERY AND RETURN:**

7.1 Delivery Time: Vendor shall deliver standard and emergency orders/services within the timelines as described in Section 3.

7.2 Late Delivery: The Agency placing the order under this Contract must be notified in writing if orders will be delayed for any reason. Any delay in delivery that could cause harm to an Agency will be grounds for cancellation of the delayed order, and/or obtaining the items ordered from a third party.

Any Agency seeking to obtain items from a third party under this provision must first obtain approval of the Purchasing Division.

7.2.1 Vendor shall refer to section 5.2.1.3 for penalties.

7.3 Delivery Payment/Risk of Loss: Standard order delivery shall be F.O.B. destination to the Agency's location. Vendor shall include the cost of standard order delivery charges in its bid pricing/discount and is not permitted to charge the Agency separately for such delivery. The Agency will pay delivery charges on all emergency orders provided that Vendor invoices those delivery costs as a separate charge with the original freight bill attached to the invoice.

7.4 Return of Unacceptable Items: If the Agency deems the Contract Items to be unacceptable, the Contract Items shall be returned to Vendor at Vendor's expense and with no restocking charge. Vendor shall either make arrangements for the return within five (5) days of being notified that items are unacceptable, or permit the Agency to arrange for the return and reimburse Agency for delivery expenses. If the original packaging cannot be utilized for the return, Vendor will supply the Agency with appropriate return packaging upon request. All returns of unacceptable items shall be F.O.B. the Agency's location. The returned product shall either be replaced, or the Agency shall receive a full credit or refund for the purchase price, at the Agency's discretion.

7.5 Return Due to Agency Error: Items ordered in error by the Agency will be returned for credit within 30 days of receipt, F.O.B. Vendor's location. Vendor shall not charge a restocking fee if returned products are in a resalable condition. Items shall be deemed to be in a resalable condition if they are unused and in the original packaging. Any restocking fee for items not in a resalable condition shall be the lower of the Vendor's customary restocking fee or 5% of the total invoiced value of the returned items.

8. **Travel:** Vendor shall be responsible for all mileage and travel costs, including travel time, associated with performance of this Contract. Any anticipated mileage or travel costs may be included in the flat fee or hourly rate listed on Vendor's bid, but such costs will not be paid by the Agency separately.

9. **VENDOR DEFAULT:**

9.1. The following shall be considered a vendor default under this Contract.

9.1.1. Failure to perform Contract Services in accordance with the requirements contained herein.

9.1.2. Failure to comply with other specifications and requirements contained herein.

9.1.3. Failure to comply with any laws, rules, and ordinances applicable to the Contract Services provided under this Contract.

9.1.4. Failure to remedy deficient performance upon request.

9.2. The following remedies shall be available to Agency upon default.

9.2.1. Immediate cancellation of the Contract.

9.2.2. Immediate cancellation of one or more release orders issued under this Contract.

9.2.3. Any other remedies available in law or equity.

Hospital Uniform Billing Data System (HUBDS)

10. MISCELLANEOUS:

10.1 No Substitutions: Vendor shall supply only Contract Items submitted in response to the Solicitation unless a contract modification is approved in accordance with the provisions contained in this Contract.

10.2 Vendor Supply: Vendor must carry sufficient inventory of the Contract Items being offered to fulfill its obligations under this Contract. By signing its bid, Vendor certifies that it can supply the Contract Items contained in its bid response.

10.3 Reports: Vendor shall provide quarterly reports and annual summaries to the Agency showing the Agency's items purchased, quantities of items purchased, and total dollar value of the items purchased. Vendor shall also provide reports, upon request, showing the items purchased during the term of this Contract, the quantity purchased for each of those items, and the total value of purchases for each of those items. Failure to supply such reports may be grounds for cancellation of this Contract. **Vendor shall refer to Section 3 for reporting requirement timelines.**

10.4 Contract Manager: During its performance of this Contract, Vendor must designate and maintain a primary contract manager responsible for overseeing Vendor's responsibilities under this Contract. The Contract manager must be available during normal business hours to address any customer service or other issues related to this Contract. Vendor should list its Contract manager and his or her contact information below.

Contract Manager: Hallie Morgan
Telephone Number: (304) 353-9714
Fax Number: (304) 414-0210
Email Address: hmorgan@wvha.org

Attachment A

FEDERAL FUNDS ADDENDUM

2 C.F.R. §§ 200.317 – 200.327

Purpose: This addendum is intended to modify the solicitation in an attempt to make the contract compliant with the requirements of 2 C.F.R. §§ 200.317 through 200.327 relating to the expenditure of certain federal funds. This solicitation will allow the State to obtain one or more contracts that satisfy standard state procurement, state federal funds procurement, and county/local federal funds procurement requirements.

Instructions: Vendors who are willing to extend their contract to procurements with federal funds and the requirements that go along with doing so, should sign the attached document identified as: "REQUIRED CONTRACT PROVISIONS FOR NON-FEDERAL ENTITY CONTRACTS UNDER FEDERAL AWARDS (2 C.F.R. § 200.317)"

Should the awarded vendor be unwilling to extend the contract to federal funds procurement, the State reserves the right to award additional contracts to vendors that can and are willing to meet federal funds procurement requirements.

Changes to Specifications: Vendors should consider this solicitation as containing two separate solicitations, one for state level procurement and one for county/local procurement.

State Level: In the first solicitation, bid responses will be evaluated with applicable preferences identified in sections 15, 15A, and 16 of the "Instructions to Vendors Submitting Bids" to establish a contract for both standard state procurements and state federal funds procurements.

County Level: In the second solicitation, bid responses will be evaluated with applicable preferences identified in Sections 15, 15A, and 16 of the "Instructions to Vendors Submitting Bids" omitted to establish a contract for County/Local federal funds procurement.

Award: If the two evaluations result in the same vendor being identified as the winning bidder, the two solicitations will be combined into a single contract award. If the evaluations result in a different bidder being identified as the winning bidder, multiple contracts may be awarded. The State reserves the right to award to multiple different entities should it be required to satisfy standard state procurement, state federal funds procurement, and county/local federal funds procurement requirements.

State Government Use Caution: State agencies planning to utilize this contract for procurements subject to the above identified federal regulations should first consult with the federal agency providing the applicable funding to ensure the contract is complaint.

County/Local Government Use Caution: County and Local government entities planning to utilize this contract for procurements subject to the above identified federal regulation should first consult with the federal agency providing the applicable funding to ensure the contract is complaint. For purposes of County/Local government use, the solicitation resulting in this contract was conducted in accordance with the procurement laws, rules, and procedures governing the West Virginia Department of Administration, Purchasing Division, except that vendor preference has been omitted for County/Local use purposes and the contract terms contained in the document entitled "REQUIRED CONTRACT PROVISIONS FOR NON-FEDERAL ENTITY CONTRACTS UNDER FEDERAL AWARDS (2 C.F.R. § 200.317)" have been added.

FEDERAL FUNDS ADDENDUM

REQUIRED CONTRACT PROVISIONS FOR NON-FEDERAL ENTITY CONTRACTS UNDER FEDERAL AWARDS (2 C.F.R. § 200.317):

The State of West Virginia Department of Administration, Purchasing Division, and the Vendor awarded this Contract intend that this Contract be compliant with the requirements of the Procurement Standards contained in the Uniform Administrative Requirements, Cost Principles, and Audit Requirements found in 2 C.F.R. § 200.317, et seq. for procurements conducted by a Non-Federal Entity. Accordingly, the Parties agree that the following provisions are included in the Contract.

1. **MINORITY BUSINESSES, WOMEN'S BUSINESS ENTERPRISES, AND LABOR SURPLUS AREA FIRMS:** (2 C.F.R. § 200.321)

    a. The State confirms that it has taken all necessary affirmative steps to assure that minority businesses, women's business enterprises, and labor surplus area firms are used when possible. Those affirmative steps include:

        (1) Placing qualified small and minority businesses and women's business enterprises on solicitation lists;
        (2) Assuring that small and minority businesses, and women's business enterprises are solicited whenever they are potential sources;
        (3) Dividing total requirements, when economically feasible, into smaller tasks or quantities to permit maximum participation by small and minority businesses, and women's business enterprises;
        (4) Establishing delivery schedules, where the requirement permits, which encourage participation by small and minority businesses, and women's business enterprises;
        (5) Using the services and assistance, as appropriate, of such organizations as the Small Business Administration and the Minority Business Development Agency of the Department of Commerce; and
        (6) Requiring the prime contractor, if subcontracts are to be let, to take the affirmative steps listed in paragraphs (1) through (5) above.

    b. Vendor confirms that if it utilizes subcontractors, it will take the same affirmative steps to assure that minority businesses, women's business enterprises, and labor surplus area firms are used when possible.

2. **DOMESTIC PREFERENCES:** (2 C.F.R. § 200.322)

    a. The State confirms that as appropriate and to the extent consistent with law, it has, to the greatest extent practicable under a Federal award, provided a preference for the purchase, acquisition, or use of goods, products, or materials produced in the United

States (including but not limited to iron, aluminum, steel, cement, and other manufactured products).

b. Vendor confirms that will include the requirements of this Section 2. Domestic Preference in all subawards including all contracts and purchase orders for work or products under this award.

c. Definitions: For purposes of this section:

(1) "Produced in the United States" means, for iron and steel products, that all manufacturing processes, from the initial melting stage through the application of coatings, occurred in the United States.
(2) "Manufactured products" means items and construction materials composed in whole or in part of non-ferrous metals such as aluminum; plastics and polymer-based products such as polyvinyl chloride pipe; aggregates such as concrete; glass, including optical fiber; and lumber.

3. **BREACH OF CONTRACT REMEDIES AND PENALTIES:**
(2 C.F.R. § 200.327 and Appendix II)

(a) The provisions of West Virginia Code of State Rules § 148-1-5 provide for breach of contract remedies, and penalties. A copy of that rule is attached hereto as Exhibit A and expressly incorporated herein by reference.

4. **TERMINATION FOR CAUSE AND CONVENIENCE:**
(2 C.F.R. § 200.327 and Appendix II)

(a) The provisions of West Virginia Code of State Rules § 148-1-5 govern Contract termination. A copy of that rule is attached hereto as Exhibit A and expressly incorporated herein by reference.

5. **EQUAL EMPLOYMENT OPPORTUNITY:**
(2 C.F.R. § 200.327 and Appendix II)

Except as otherwise provided under 41 CFR Part 60, and if this contract meets the definition of "federally assisted construction contract" in 41 CFR Part 60–1.3, this contract includes the equal opportunity clause provided under 41 CFR 60–1.4(b), in accordance with Executive Order 11246, "Equal Employment Opportunity" (30 FR 12319, 12935, 3 CFR Part, 1964–1965 Comp., p. 339), as amended by Executive Order 11375, "Amending Executive Order 11246 Relating to Equal Employment Opportunity," and implementing regulations at 41 CFR part 60, "Office of Federal Contract Compliance Programs, Equal Employment Opportunity, Department of Labor."

6. **DAVIS-BACON WAGE RATES:**
(2 C.F.R. § 200.327 and Appendix II)

Vendor agrees that if this Contract includes construction, all construction work in excess of $2,000 will be completed and paid for in compliance with the Davis–Bacon Act (40 U.S.C. 3141–3144, and 3146–3148) as supplemented by Department of Labor regulations (29 CFR Part 5, "Labor Standards Provisions Applicable to Contracts Covering Federally Financed and Assisted Construction"). In accordance with the statute, contractors must:

(a) pay wages to laborers and mechanics at a rate not less than the prevailing wages specified in a wage determination made by the Secretary of Labor.
(b) pay wages not less than once a week.

A copy of the current prevailing wage determination issued by the Department of Labor is attached hereto as Exhibit B. The decision to award a contract or subcontract is conditioned upon the acceptance of the wage determination. The State will report all suspected or reported violations to the Federal awarding agency.

7. **ANTI-KICKBACK ACT:**
(2 C.F.R. § 200.327 and Appendix II)

Vendor agrees that it will comply with the Copeland Anti-KickBack Act (40 U.S.C. 3145), as supplemented by Department of Labor regulations (29 CFR Part 3, "Contractors and Subcontractors on Public Building or Public Work Financed in Whole or in Part by Loans or Grants from the United States"). Accordingly, Vendor, Subcontractors, and anyone performing under this contract are prohibited from inducing, by any means, any person employed in the construction, completion, or repair of public work, to give up any part of the compensation to which he or she is otherwise entitled. The State must report all suspected or reported violations to the Federal awarding agency.

8. **CONTRACT WORK HOURS AND SAFETY STANDARDS ACT**
(2 C.F.R. § 200.327 and Appendix II)

Where applicable, and only for contracts awarded by the State in excess of $100,000 that involve the employment of mechanics or laborers, Vendor agrees to comply with 40 U.S.C. 3702 and 3704, as supplemented by Department of Labor regulations (29 CFR Part 5). Under 40 U.S.C. 3702 of the Act, Vendor is required to compute the wages of every mechanic and laborer on the basis of a standard work week of 40 hours. Work in excess of the standard work week is permissible provided that the worker is compensated at a rate of not less than one and a half times the basic rate of pay for all hours worked in excess of 40 hours in the work week. The requirements of 40 U.S.C. 3704 are applicable to construction work and provide that no laborer or mechanic must be required to work in surroundings or under working conditions which are unsanitary, hazardous or dangerous. These requirements do not apply to the purchases of supplies or materials or articles ordinarily available on the open market, or contracts for transportation or transmission of intelligence.

9. **RIGHTS TO INVENTIONS MADE UNDER A CONTRACT OR AGREEMENT.**
(2 C.F.R. § 200.327 and Appendix II)

If the Federal award meets the definition of "funding agreement" under 37 CFR § 401.2 (a) and the recipient or subrecipient wishes to enter into a contract with a small business firm or nonprofit organization regarding the substitution of parties, assignment or performance of experimental, developmental, or research work under that "funding agreement," the recipient or subrecipient must comply with the requirements of 37 CFR Part 401, "Rights to Inventions Made by Nonprofit Organizations and Small Business Firms Under Government Grants, Contracts and Cooperative Agreements," and any implementing regulations issued by the awarding agency.

10. **CLEAN AIR ACT**
(2 C.F.R. § 200.327 and Appendix II)

Vendor agrees that if this contract exceeds $150,000, Vendor is to comply with all applicable standards, orders or regulations issued pursuant to the Clean Air Act (42 U.S.C. 7401–7671q) and the Federal Water Pollution Control Act as amended (33 U.S.C. 1251–1387). Violations must be reported to the Federal awarding agency and the Regional Office of the Environmental Protection Agency (EPA).

11. **DEBARMENT AND SUSPENSION**
(2 C.F.R. § 200.327 and Appendix II)

The State will not award to any vendor that is listed on the governmentwide exclusions in the System for Award Management (SAM), in accordance with the OMB guidelines at 2 CFR 180 that implement Executive Orders 12549 (3 CFR part 1986 Comp., p. 189) and 12689 (3 CFR part 1989 Comp., p. 235), "Debarment and Suspension." SAM Exclusions contains the names of parties debarred, suspended, or otherwise excluded by agencies, as well as parties declared ineligible under statutory or regulatory authority other than Executive Order 12549.

12. **BYRD ANTI–LOBBYING AMENDMENT**
(2 C.F.R. § 200.327 and Appendix II)

Vendors that apply or bid for an award exceeding $100,000 must file the required certification. Each tier certifies to the tier above that it will not and has not used Federal appropriated funds to pay any person or organization for influencing or attempting to influence an officer or employee of any agency, a member of Congress, officer or employee of Congress, or an employee of a member of Congress in connection with obtaining any Federal contract, grant or any other award covered by 31 U.S.C. 1352. Each tier must also disclose any lobbying with non–Federal funds that takes place in connection with obtaining any Federal award. Such disclosures are forwarded from tier to tier up to the non–Federal award.

13. **PROCUREMENT OF RECOVERED MATERIALS**
(2 C.F.R. § 200.327 and Appendix II; 2 C.F.R. § 200.323)

Vendor agrees that it and the State must comply with section 6002 of the Solid Waste Disposal Act, as amended by the Resource Conservation and Recovery Act. The requirements of Section 6002 include procuring only items designated in guidelines of the

Environmental Protection Agency (EPA) at 40 CFR part 247 that contain the highest percentage of recovered materials practicable, consistent with maintaining a satisfactory level of competition, where the purchase price of the item exceeds $10,000 or the value of the quantity acquired during the preceding fiscal year exceeded $10,000; procuring solid waste management services in a manner that maximizes energy and resource recovery; and establishing an affirmative procurement program for procurement of recovered materials identified in the EPA guidelines.

14. PROHIBITION ON CERTAIN TELECOMMUNICATIONS AND VIDEO SURVEILLANCE SERVICES OR EQUIPMENT.
(2 C.F.R. § 200.327 and Appendix II; 2 CFR § 200.216)

Vendor and State agree that both are prohibited from obligating or expending funds under this Contract to:

(1) Procure or obtain;
(2) Extend or renew a contract to procure or obtain; or
(3) Enter into a contract (or extend or renew a contract) to procure or obtain equipment, services, or systems that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. As described in Public Law 115–232, section 889, covered telecommunications equipment is telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliate of such entities).

(i) For the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes, video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of such entities).
(ii) Telecommunications or video surveillance services provided by such entities or using such equipment.
(iii) Telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of the National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country.

In implementing the prohibition under Public Law 115–232, section 889, subsection (f), paragraph (1), heads of executive agencies administering loan, grant, or subsidy programs shall prioritize available funding and technical support to assist affected businesses, institutions and organizations as is reasonably necessary for those affected entities to transition from covered communications equipment and services, to procure replacement equipment and services, and to ensure that communications service to users and customers is sustained.

State of West Virginia

By: Heather White

Printed Name: Heather White

Title: Procurement Specialist, Senior

Date: 3/11/24

Vendor Name:

By: M. J. Kaufman

Printed Name: M. JAMES KAUFMAN

Title: PRESIDENT & CEO

Date: 2/23/24

EXHIBIT A To:
REQUIRED CONTRACT PROVISIONS FOR NON-FEDERAL ENTITY CONTRACTS UNDER FEDERAL AWARDS (2 C.F.R. § 200.317):

W. Va. CSR § 148-1-5

West Virginia Code of State Rules
Title 148. Department of Administration
Legislative Rule (Ser. 1)
Series 1. Purchasing

W. Va. Code St. R. § 148-1-5

§ 148-1-5. Remedies.

Currentness

5.1. The Director may require that the spending unit attempt to resolve any issues that it may have with the vendor prior to pursuing a remedy contained herein. The spending unit must document any resolution efforts and provide copies of those documents to the Purchasing Division.

5.2. Contract Cancellation.

5.2.1. Cancellation. The Director may cancel a purchase or contract immediately under any one of the following conditions including, but not limited to:

5.2.1.a. The vendor agrees to the cancellation;

5.2.1.b. The vendor has obtained the contract by fraud, collusion, conspiracy, or is in conflict with any statutory or constitutional provision of the State of West Virginia;

5.2.1.c. Failure to honor any contractual term or condition or to honor standard commercial practices;

5.2.1.d. The existence of an organizational conflict of interest is identified;

5.2.1.e. Funds are not appropriated or an appropriation is discontinued by the legislature for the acquisition;

5.2.1.f. Violation of any federal, state, or local law, regulation, or ordinance, and

5.2.1.g. The contract was awarded in error.

5.2.2. The Director may cancel a purchase or contract for any reason or no reason, upon providing the vendor with 30 days' notice of the cancellation.

5.2.3. Opportunity to Cure. In the event that a vendor fails to honor any contractual term or condition, or violates any provision of federal, state, or local law, regulation, or ordinance, the Director may request that the vendor remedy the contract breach or legal violation within a time frame the Director determines to be appropriate. If the vendor fails to remedy the contract breach or legal violation or the Director determines, at his or her sole discretion, that such a request is unlikely to yield a satisfactory result, then he or she may cancel immediately without providing the vendor an opportunity to perform a remedy.

5.2.4. Re-Award. The Director may award the cancelled contract to the next lowest responsible bidder (or next highest scoring bidder if best value procurement) without a subsequent solicitation if the following conditions are met:

5.2.4.a. The next lowest responsible bidder (or next highest scoring bidder if best value procurement) is able to perform at the price contained in its original bid submission, and

5.2.4.b. The contract is an open-end contract, a one-time purchase contract, or a contract for work which has not yet commenced.

Award to the next lowest responsible bidder (or next highest scoring bidder if best value procurement) will not be an option if the vendor's failure has in any way increased or significantly changed the scope of the original contract. The vendor failing to honor contractual and legal obligations is responsible for any increase in cost the state incurs as a result of the re-award.

5.3. Non-Responsible. If the Director believes that a vendor may be non-responsible, the Director may request that a vendor or spending unit provide evidence that the vendor either does or does not have the capability to fully perform the contract requirements, and the integrity and reliability necessary to assure good faith performance. If the Director determines that the vendor is non-responsible, the Director shall reject that vendor's bid and shall not award the contract to that vendor. A determination of non-responsibility must be evaluated on a case-by-case basis and can only be made after the vendor in question has submitted a bid. A determination of non-responsibility will only extend to the contract for which the vendor has submitted a bid and does not operate as a bar against submitting future bids.

5.4. Suspension.

5.4.1. The Director may suspend, for a period not to exceed 1 year, the right of a vendor to bid on procurements issued by the Purchasing Division or any state spending unit under its authority if:

5.4.1.a. The vendor has submitted a bid and then requested that its bid be withdrawn after bids have been publicly opened.

5.4.1.b. The vendor has exhibited poor performance in fulfilling his or her contractual obligations to the State. Poor performance includes, but is not limited to any of the following: violations of law, regulation, or ordinance; failure to deliver timely; failure to deliver quantities ordered; poor performance reports; or failure to deliver commodities, services, or printing at the quality level required by the contract.

5.4.1.c. The vendor has breached a contract issued by the Purchasing Division or any state spending unit under its authority and refuses to remedy that breach.

5.4.1.d. The vendor's actions have given rise to one or more of the grounds for debarment listed in W. Va. Code § 5A-3-33d.

5.4.2. Vendor suspension for the reasons listed in section 5.4 above shall occur as follows:

5.4.2.a. Upon a determination by the Director that a suspension is warranted, the Director will serve a notice of suspension to the vendor.

5.4.2.b. A notice of suspension must inform the vendor:

5.4.2.b.1. Of the grounds for the suspension;

5.4.2.b.2. Of the duration of the suspension;

5.4.2.b.3. Of the right to request a hearing contesting the suspension;

5.4.2.b.4. That a request for a hearing must be served on the Director no later than 5 working days of the vendor's receipt of the notice of suspension;

5.4.2.b.5. That the vendor's failure to request a hearing no later than 5 working days of the receipt of the notice of suspension will be deemed a waiver of the right to a hearing and result in the automatic enforcement of the suspension without further notice or an opportunity to respond; and

5.4.2.b.6. That a request for a hearing must include an explanation of why the vendor believes the Director's asserted grounds for suspension do not apply and why the vendor should not be suspended.

5.4.2.c. A vendor's failure to serve a request for hearing on the Director no later than 5 working days of the vendor's receipt of the notice of suspension will be deemed a waiver of the right to a hearing and may result in the automatic enforcement of the suspension without further notice or an opportunity to respond.

5.4.2.d. A vendor who files a timely request for hearing but nevertheless fails to provide an explanation of why the asserted grounds for suspension are inapplicable or should not result in a suspension, may result in a denial of the vendor's hearing request.

5.4.2.e. Within 5 working days of receiving the vendor's request for a hearing, the Director will serve on the vendor a notice of hearing that includes the date, time and place of the hearing.

5.4.2.f. The hearing will be recorded and an official record prepared. Within 10 working days of the conclusion of the hearing, the Director will issue and serve on the vendor, a written decision either confirming or reversing the suspension.

5.4.3. A vendor may appeal a decision of the Director to the Secretary of the Department of Administration. The appeal must be in writing and served on the Secretary no later than 5 working days of receipt of the Director's decision.

5.4.4. The Secretary, or his or her designee, will schedule an appeal hearing and serve on the vendor, a notice of hearing that includes the date, time and place of the hearing. The appeal hearing will be recorded and an official record prepared. Within 10 working days of the conclusion of the appeal hearing, the Secretary will issue and serve on the vendor a written decision either confirming or reversing the suspension.

5.4.5. Any notice or service related to suspension actions or proceedings must be provided by certified mail, return receipt requested.

5.5. Vendor Debarment. The Director may debar a vendor on the basis of one or more of the grounds for debarment contained in W. Va. Code § 5A-3-33d or if the vendor has been declared ineligible to participate in procurement related activities under federal laws and regulation.

5.5.1. Debarment proceedings shall be conducted in accordance with W. Va. Code § 5A-3-33e and these rules. A vendor that has received notice of the proposed debarment by certified mail, return receipt requested, must respond to the proposed debarment within 30 working days after receipt of notice or the debarment will be instituted without further notice. A vendor is deemed to have received notice, notwithstanding the vendor's failure to accept the certified mail, if the letter is addressed to the vendor at its last known address. After considering the matter and reaching a decision, the Director shall notify the vendor of his or her decision by certified mail, return receipt requested.

5.5.2. Any vendor, other than a vendor prohibited from participating in federal procurement, undergoing debarment proceedings is permitted to continue participating in the state's procurement process until a final debarment decision has been reached. Any contract that a debarred vendor obtains prior to a final debarment decision shall remain in effect for the current term, but may not be extended or renewed. Notwithstanding the foregoing, the Director may cancel a contract held by a debarred vendor if the Director determines, in his or her sole discretion, that doing so is in the best interest of the State. A vendor prohibited from participating in federal procurement will not be permitted to participate in the state's procurement process during debarment proceedings.

5.5.3. If the Director's final debarment decision is that debarment is warranted and notice of the final debarment decision is mailed, the Purchasing Division shall reject any bid submitted by the debarred vendor, including any bid submitted prior to the final debarment decision if that bid has not yet been accepted and a contract consummated.

5.5.4. Pursuant to W.Va. Code § 5A-3-33e(e), the length of the debarment period will be specified in the debarment decision and will be for a period of time that the Director finds necessary and proper to protect the public from an irresponsible vendor.

5.5.5. List of Debarred Vendors. The Director shall maintain and publicly post a list of debarred vendors on the Purchasing Division's website.

5.5.6. Related Party Debarment. The Director may pursue debarment of a related party at the

same time that debarment of the original vendor is proceeding or at any time thereafter that the Director determines a related party debarment is warranted. Any entity that fails to provide the Director with full, complete, and accurate information requested by the Director to determine related party status will be presumed to be a related party subject to debarment.

5.6. Damages.

5.6.1. A vendor who fails to perform as required under a contract shall be liable for actual damages and costs incurred by the state.

5.6.2. If any commodities delivered under a contract have been used or consumed by a spending unit and on testing the commodities are found not to comply with specifications, no payment may be approved by the Spending Unit for the merchandise until the amount of actual damages incurred has been determined.

5.6.3. The Spending Unit shall seek to collect damages by following the procedures established by the Office of the Attorney General for the collection of delinquent obligations.

Credits

History: Filed 4-1-19, eff. 4-1-19; Filed 4-16-21, eff. 5-1-21.

Current through register dated May 7, 2021. Some sections may be more current. See credits for details.
W. Va. C.S.R. § 148-1-5, WV ADC § 148-1-5

End of Document

EXHIBIT B To:
REQUIRED CONTRACT PROVISIONS FOR NON-FEDERAL ENTITY CONTRACTS UNDER FEDERAL AWARDS (2 C.F.R. § 200.317):

Prevailing Wage Determination

[ ] – Not Applicable Because Contract Not for Construction

[ ] – Federal Prevailing Wage Determination on Next Page

Attachment B

WEST VIRGINIA Department of Health & Human Resources

WEST VIRGINIA HEALTHCARE AUTHORITY

West Virginia

Hospital Data Submission System

Data Element Specifications Guide

West Virginia Hospital Association

January 2020

Introduction

The West Virginia Hospital Data Submission System (HDSS) collects, processes, and analyzes inpatient and outpatient discharge data that are collected by the West Virginia Health Care Authority (WVHCA). This Guide outlines specifications for the data elements that are required to be submitted to the WVHCA/WVDHHR by all non-federal hospitals in the state. The table below defines the information that is contained in the data element tables presented in this Guide.

Refer to the *Data Collection Policies and Procedures* guide for hospital inpatient data reporting requirements. Additional technical documents are available to provide specific details regarding the data file layout and submission procedures. All data reporting and technical documentation can be accessed from the WVHCA website (http://www.hca.wv.gov/fdhome/HospInpatientData) or from the Hospital Data Submission System (HDSS) (https://www.hidionline.com/HIDINetV3/).

Data Element Specification Table Layout

Data Element Name

Description	A description or definition of the data element.
837i Guide	WVHDSS File Specifications 837i Companion Guide corresponding page number
UB-04 Element	Reference to the UB-04 Form Locator.
HDSS Field	Name of the data element as it appears in the West Virginia Hospital Data Submission System.
Format & Valid Codes	A description of the required format and accepted codes.
Edit Check Errors & Warnings	A list of the errors and/or warnings that may appear in the Hospital Data Submission System as a result of the edits checks performed on the data element. Fatal errors on inpatient records must be corrected before data may be considered complete. Outpatient records are considered complete and do not require corrections if overall fatal error rate is less than 5%.
Notes	Any special data submission or processing notes related to the data element.

Alphabetical Index of Data Elements

This table presents an alphabetical list of the data elements, their abbreviated field name in the Hospital Data Submission System (HDSS), and the page number of the corresponding data element specifications table in this Guide.

Alphabetical Index of Data Elements

Admission Date & Time

Description	Date & Time of admission to hospital
837i Guide	Page 3
UB-04 Element	FL 12 & 13
HDSS Field	Admit Date
Format & Valid Codes	Date formatted as specified in the *WVHDSS File Specifications 837i Companion Guide*
Edit Check *Fatal Errors*	• 1101 = Admit date is missing (no error on Outpatients) • 1102 = Admit date is invalid • 1103 = Admit date is greater than discharge date
Notes	Admission date is formatted as CCYYMMDDHHMM.

Admission Type Code/Priority of Visit

Description	Code indicating the priority (type) of admission
837i Guide	Page 3
UB-04 Element	FL 14
HDSS Field	Admit Type
Format & Valid Codes	Submit valid codes per NUBC Official UB-04 Data Specifications
Edit Check *Fatal Errors*	• 2801 = Priority of visit is missing • 2802 = Priority of visit is invalid • 2805 = Priority of visit newborn, birthdate prior to Admit date
Notes	1. For births occurring in the hospital, the admission type should be coded as '4.' This code requires the use of the newborn codes for source of admission. 2. In accordance with WVHCA *Data Collection Policies and Procedures*, separate discharge records should be submitted for newborns and mothers.

Admit from Emergency Room Condition Code

Description	Code indicating patient admitted directly from facility's Emergency Room/Dept. (Inpatient only)
837i Guide	Page 3
UB-04 Element	FL 18-28
HDSS Field	Condition Code
Format & Valid Codes	Submit a "P7" per NUBC Official UB-04 Data Specifications if the patient was admitted as an inpatient directly from the emergency room/department.
Edit Check *Fatal Errors*	• 7102 = Condition code is invalid (Inpatient Only) • 7103 = Condition code P7 reported, no 45x revenue code reported (Inpatient Only)
Notes	

Admitting Diagnosis Code

Description	Code indicating the diagnosis at the time of admission (Inpatient only)
837i Guide	Page 3
UB-04 Element	FL 69
HDSS Field	Admit Diagnosis
Format & Valid Codes	ICD-10-CM Codes
Edit Check *Fatal Errors*	• 4501 = Admit DX is missing (Inpatient only) • 4502 = Admit DX is invalid (Inpatient only)
Notes	

Auto Accident State Code

Description	State abbreviation code where the auto accident occurred
837i Guide	Page 3
UB-04 Element	FL 29
HDSS Field	Acc. State
Format & Valid Codes	Two-digit state abbreviation
Edit Check *Fatal Errors*	
Notes	Required when the services reported on the claim are related to an auto accident.

Bill Type Code

Description	Code indicating the specific type of bill
837i Guide	Page 3
UB-04 Element	FL 04
HDSS Field	Bill Type
Format & Valid Codes	Submit valid codes per NUBC Official UB-04 Data Specifications. **All Hospital Inpatient and Outpatient visits** should be reported EXCEPT skilled nursing and long-term care discharges.
Edit Check *Fatal Errors*	• 4101 = Bill type is missing • 4102 = Bill type is invalid
Notes	The 837 format requires the bill type code to be submitted in two fields. It is displayed as one field in the HDSS.

External Cause of Injury Code

Description	Code pertaining to external cause of injuries, poisoning, or adverse effect
837i Guide	Page 4
UB-04 Element	FL 72a-c
HDSS Field	Diagnosis Codes – ECM Code
Format & Valid Codes	ICD-10-CM Codes
Edit Check *Fatal Errors*	
Notes	• Required when an injury, poisoning, or adverse effect is the cause for seeking medical treatment.

External Cause of Injury POA Code

Description	Code indicating present on admission status of external cause of injuries, poisoning, or adverse effect
837I Element	Page 5
UB-04 Element	FL 72a-c
HDSS Field	EPOA
Format & Valid Codes	**Refer to the 837I documentation for details regarding the format of the POA field.* **Refer to ICD-10-CM Official Guidelines for additional code descriptions and instructions.* Y = Yes (Present at the time of inpatient admission) N = No (Not present at the time of inpatient admission) U = No information in the record (Documentation is insufficient to determine if condition was present on admission or not) W = Clinically Undetermined (Provider is unable to clinically determine whether condition was present on admission or not) Blank/null = Unreported/not used (Exempt from POA reporting)
Edit Check *Fatal Errors*	• 5002 = ECM POA is invalid (Inpatient only)
Notes	Per ICD-10-CM and CMS guidelines, some hospitals and diagnosis codes are exempt from POA reporting. Medicare Provider numbers with the first 3 digits of 511, 512, 513, 514, 515, 51S, 51T, 51U, or 51Z are exempt. Although it is not required, exempt hospitals are strongly encouraged to submit POA information to the WVHCA.

HCPCS/CPT Code

Description	Code used to represent medical procedures and services provided
837i Guide	Page 4
UB-04 Element	FL 44
HDSS Field	Revenue Codes - HCPCS
Format & Valid Codes	HCPCS
Edit Check *Fatal Errors*	
Notes	1. Healthcare Common Procedure Coding System (HCPCS) is a set of health care procedure codes based on CPT (Current Procedural Terminology). 2. Required in outpatient records only

Medical Record Number

Description	Number assigned to the patient's medical/health record by the provider
837i Guide	Page 4
UB-04 Element	FL 03b
HDSS Field	Medical Record Number
Format & Valid Codes	No standard format required
Edit Check *Fatal Errors*	• 301 = Medical record number is missing
Notes	The patient control number identifies a single episode of care; the medical record number identifies a patient across multiple episodes of care.

Medicare Provider Number (CMS Certification Number/PTAN)

Description	Medicare provider identification number indicating the type of service (Inpatient only)
837i Guide	Page 4
UB-04 Element	N/A
HDSS Field	Medicare No.
Format & Valid Codes	Six-digit Medicare certification number issued by CMS specific to type of hospital service/unit including: Acute Critical Access Long Term Acute Care Rehabilitation Psychiatric Swing
Edit Check *Fatal Errors*	• 6001 = Medicare number is missing (Inpatient only) • 6002 = Medicare number is invalid (Inpatient only) • 6003 = Medicare number doesn't match bill type (Inpatient only)
Notes	This number is assigned by the Centers for Medicare & Medicaid Services (CMS) Division of Survey & Certifications.

NPI Attending Physician

Description	Unique national provider identification number assigned to the attending provider
837i Guide	Page 4
UB-04 Element	FL 76
HDSS Field	Attending
Format & Valid Codes	10-character National Provider Identifier
Edit Check *Fatal Errors*	• 2601 = Attending physician missing
Notes	The attending provider is the individual who had overall responsibility for the patient's medical care and treatment reported in the claim.

NPI Billing Provider

Description	Unique national provider identification number assigned to the provider submitting the bill
837i Guide	Page 4
UB-04 Element	FL 56
HDSS Field	NPI
Format & Valid Codes	10-character National Provider Identifier
Edit Check *Fatal Errors*	• 6301 = Facility NPI is missing • 6302 = Facility NPI is invalid • 6303 = Facility NPI is not on file
Notes	

NPI Operating Physician

Description	Unique national provider identification number assigned to the operating physician
837i Guide	Page 4
UB-04 Element	FL 77
HDSS Field	Operating
Format & Valid Codes	10-character National Provider Identifier
Edit Check *Fatal Errors*	
Notes	The operating physician is the individual with the primary responsibility for performing the surgical procedure(s).

NPI Other Physician(s) (Includes Rendering Provider)

Description	Unique national provider identification number assigned to other physicians involved in care
837I Guide	Page 4, 5
UB-04 Element	FL 78, FL 79
HDSS Field	NPI_OTH1, NPI_OTH2, NPI_REND
Format & Valid Codes	10-character National Provider Identifier
Edit Check *Fatal Errors*	
Notes	NPIs for two additional physicians can be submitted.

Other Diagnosis Code(s)

Description	Codes corresponding to additional/secondary conditions related to the admission
837I Guide	Page 4
UB-04 Element	FL 67A-Q
HDSS Field	Diagnosis Codes – Diagnosis Code (not listed first)
Format & Valid Codes	ICD-10-CM Diagnosis Codes
Edit Check *Fatal Errors*	• 1504 = Other DX is invalid • 1522 = Other DX is duplicated of principal DX • 1523 = Duplicate secondary diagnosis reported
Notes	1. Report additional conditions that coexist at the time of admission, that develop subsequently, or that affect the treatment received and/or the length of stay. 2. Up to 24 secondary diagnosis codes can be submitted.

Other Procedure Code(s)

Description	Codes identifying additional significant procedures performed during the service period
837I Guide	Page 6
UB-04 Element	FL 74a-e
HDSS Field	Procedure Codes – Procedure Code (not listed first)
Format & Valid Codes	ICD-10-CM Procedure Codes
Edit Check *Fatal Errors*	• 1603 = Other PX is invalid • 1607 = Other PX date, but no other PX
Notes	Report all (up to 12) additional procedures that were most important for the episode of care and specifically any therapeutic procedures closely related to the principal diagnosis.

Other Procedure Dates

Description	Dates corresponding to other procedure codes
837i Guide	Page 7
UB-04 Element	FL 74 a-e
HDSS Field	Procedure Codes – Procedure Date (not listed first)
Format & Valid Codes	Dates formatted as specified in the *WVHDSS File Specifications 837I Companion Guide*
Edit Check *Fatal Errors*	• 1702 = Other PX date is missing • 1708 = Other PX date is not between stmt from date and discharge date (Inpatient only)
Notes	

Patient Address Line

Description	Patient address line, street address or PO Box
837I Guide	Page 5
UB-04 Element	FL 09
HDSS Field	Address
Format & Valid Codes	Submit street address per NUBC Official UB-04 Data Specifications
Edit Check *Fatal Errors*	
Notes	

Patient Birth Date

Description	Date of birth of the patient
837i Guide	Page 5
UB-04 Element	FL 10
HDSS Field	Birth Date
Format & Valid Codes	Date formatted as YYYYMMDD
Edit Check *Fatal Errors*	• 701 = Birthdate is invalid • 702 = Birthdate is missing • 703 = Birthdate is greater than Admit date • 2805 = Priority of visit newborn, birthdate prior to Admit date
Notes	

Patient City Name

Description	Patient address line, city name
837i Guide	Page 5
UB-04 Element	FL 09
HDSS Field	City
Format & Valid Codes	Submit city name per NUBC Official UB-04 Data Specifications
Edit Check *Fatal Errors*	
Notes	This field will not be visible or editable on the HDSS, and it will not appear on any reports.

Patient Control Number

Description	Unique identification number assigned to each discharge
837i Guide	Page 5
UB-04 Element	FL 03a
HDSS Field	Patient Control Number
Format & Valid Codes	No standard format required. However, the patient control number is used as the record key and if it is missing the record will be skipped and not counted.
Edit Check *Fatal Errors*	
Notes	The patient control number must be unique to each discharge

Patient First Name

Description	First name of the patient
837i Guide	Page 5
UB-04 Element	FL 08
HDSS Field	First Name
Format & Valid Codes	Submit per NUBC Official UB-04 Data Specifications
Edit Check *Fatal Errors*	
Notes	

Patient Last Name

Description	Last name of the patient
837i Guide	Page 5
UB-04 Element	FL 08
HDSS Field	Last Name
Format & Valid Codes	Submit per NUBC Official UB-04 Data Specifications
Edit Check *Fatal Errors*	
Notes	

Patient Gender Code

Description	Sex of the patient as recorded at admission
837i Guide	Page 5
UB-04 Element	FL 11
HDSS Field	Sex
Format & Valid Codes	M = Male F = Female U = Unknown
Edit Check *Fatal Errors*	• 501 = Sex is invalid • 502 = Sex is missing
Notes	

Patient Name Suffix

Description	Patient name suffix
837i Guide	Page 5
UB-04 Element	FL 08
HDSS Field	Suffix
Format & Valid Codes	Submit per NUBC Official UB-04 Data Specifications
Edit Check *Fatal Errors*	
Notes	

Patient Race & Ethnicity Code

Description	Race and ethnicity as reported by the patient
837i Guide	Page 5
UB-04 Element	N/A
HDSS Field	Race
Format & Valid Codes	Submit WVHCA valid codes as outlined below. 1 = White and Non-Hispanic 2 = White and Hispanic/Latino 3 = White and Unknown Ethnicity 4 = Black and Non-Hispanic 5 = Black and Hispanic/Latino 6 = Black and Unknown Ethnicity 7 = Asian 8 = Native Hawaiian or Other Pacific Islander 9 = American Indian or Alaska Native M = Multiple Races and Non-Hispanic R = Multiple Races and Hispanic/Latino S = Multiple Races and Unknown Ethnicity T = Unknown Race and Hispanic/Latino Y = Other U = Unknown
Edit Check *Fatal Errors*	• 601 = Race is invalid • 602 = Race is missing
Notes	New race and ethnicity codes were required with the implementation of the WVHCA 837i 4010 file format. They are continued with the 837i 5010 file format.

Patient State

Description	Patient address line, state abbreviation
837i Guide	Page 6
UB-04 Element	FL 09
HDSS Field	State
Format & Valid Codes	Submit state per NUBC Official UB-04 Data Specifications
Edit Check *Fatal Errors*	
Notes	

Patient (Discharge) Status Code

Description	Code indicating the status of the patient at the end of the service period covered on this bill
837i Guide	Page 6
UB-04 Element	FL 17
HDSS Field	Discharge Status
Format & Valid Codes	Submit valid codes per NUBC Official UB-04 Data Specifications
Edit Check *Fatal Errors*	• 1001 = Patient disposition is invalid • 1002 = Patient disposition is missing • 1003 = Patient disposition is invalid for inpatient (inpatient only)
Notes	

Patient Zip Code

Description	Zip code where the patient resides
837i Guide	Page 6
UB-04 Element	FL 09 subset
HDSS Field	Zip
Format & Valid Codes	Five-digit postal zip code
Edit Check *Fatal Errors*	• 2001 = Zip code is missing • 2002 = Zip code is invalid
Notes	

Payer Code(s)

Description	Codes indicating the primary, secondary, and tertiary payers billed for the service
837i Guide	Page 6
UB-04 Element	FL 50
HDSS Field	Payers - Code
Format & Valid Codes	Submit WVHCA payer codes as defined in the *WVHCA Payer Coding Specifications*
Edit Check *Fatal Errors*	• 401 = Primary payer is invalid • 402 = Primary payer is missing • 403 = Payer is invalid
Notes	Secondary and tertiary payer codes are required to be submitted when other payers are known to potentially be involved in paying the claim.

Point of Origin (Admission Source Code)

Description	Code indicating the point of patient origin for the admission
837i Guide	Page 6
UB-04 Element	FL 15
HDSS Field	Admit Source
Format & Valid Codes	Submit valid codes per NUBC Official UB-04 Data Specifications
Edit Check *Fatal Errors*	• 2201 = Point of origin is missing • 2202 = Point of origin is invalid • 2203 = Point of origin is invalid for newborn
Notes	In accordance with WVHCA *Data Collection Policies and Procedures*, separate discharge records should be submitted for newborns and mothers. If Admit Type = 4 then Admit Source must be 5 or 6.

Present on Admission (POA) Code(s)

Description	Present on admission code corresponding to a diagnosis code (Inpatient only)
837i Guide	Page 6
UB-04 Element	FL 67, FL67 A-Q
HDSS Field	Diagnosis Codes - POA
Format & Valid Codes	**Refer to the 837i documentation for details regarding the format of the POA field.* **Refer to ICD-10-CM Official Guidelines for additional code descriptions and instructions.* Y = Yes (Present at the time of inpatient admission) N = No (Not present at the time of inpatient admission) U = No information in the record (Documentation is insufficient to determine if condition was present on admission or not) W = Clinically Undetermined (Provider is unable to clinically determine whether condition was present on admission or not) Blank/null = Unreported/not used (Exempt from POA reporting)
Edit Check *Fatal Errors*	• 1301 = Principal DX POA is missing (Inpatient only) • 1302 = Principal DX POA is invalid (Inpatient only) • 1304 = Other DX POA is missing (Inpatient only) • 1305 = Other DX POA is invalid (Inpatient only) • 1309 = Principal DX POA is invalid, DX code exempt (Inpatient only) • 1310 = Other DX POA is invalid, DX code exempt (Inpatient only)
Notes	Per ICD-10-CM and CMS guidelines, some hospitals and diagnosis codes are exempt from POA reporting. Medicare Provider numbers with the first 3 digits of 511, 512, 513, 514, 515, 51S, 51T, 51U, or 51Z are exempt. Although it is not required, exempt hospitals are strongly encouraged to submit POA information.

Principal Diagnosis Code

Description	Code indicating the condition determined to be chiefly responsible for the admission
837i Guide	Page 4
UB-04 Element	FL 67
HDSS Field	Diagnosis Codes – Diagnosis Code (listed first)
Format & Valid Codes	ICD-10-CM Diagnosis Codes
Edit Check Fatal Errors	• 1501 = Principal DX missing • 1502 = Principal Dx invalid • 1505 = ECM code is invalid as principal DX
Notes	

Principal Procedure Code

Description	Code identifying the inpatient principal procedure performed during the service period
837i Guide	Page 6
UB-04 Element	FL 74
HDSS Field	Procedure Codes – Procedure Code (listed first)
Format & Valid Codes	ICD-10-CM Procedure Codes
Edit Check *Fatal Errors*	• 1602 = Principal PX is invalid • 1606 = Principal PX date, but no principal PX
Notes	• Required when a procedure was performed.

Principal Procedure Date

Description	Date corresponding to the principal procedure code
837i Guide	Page 7
UB-04 Element	FL 74
HDSS Field	Procedure Codes – Procedure Date (listed first)
Format & Valid Codes	Dates formatted as specified in the *WVHDSS File Specifications 837i Companion Guide*
Edit Check *Fatal Errors*	• 1701 = Principal PX date is missing • 1707 = Principal PX date is not between stmt from date and discharge date (Inpatient only)
Notes	

Revenue Codes

Description	Codes identifying specific accommodation and ancillary services provided
837I Guide	Page 7
UB-04 Element	FL 42
HDSS Field	Revenue Codes - Code
Format & Valid Codes	Submit valid codes per NUBC Official UB-04 Data Specifications
Edit Check *Fatal Errors*	• 3701 = Revenue code is missing • 3702 = Revenue code is invalid • 3711 = More than 999 revenue line items
Notes	A maximum of 999 revenue codes and corresponding units/charges may be submitted.

Revenue Units

Description	Service quantity pertaining to the corresponding revenue code
837i Guide	Page 7
UB-04 Element	FL 46
HDSS Field	Revenue Codes – Units
Format & Valid Codes	Number of units
Edit Check *Fatal Errors*	• 3801 = Revenue units missing • 3802 = Revenue units non-numeric • 3803 = Revenue units are negative
Notes	A maximum of 999 revenue codes and corresponding units/charges may be submitted.

Revenue Charges

Description	Total charges pertaining to the corresponding revenue code
837i Guide	Page 7
UB-04 Element	FL 47
HDSS Field	Revenue Code - Charge
Format & Valid Codes	Dollar amount – 15-character max (including decimal point). If the decimal point is not submitted, it will be interpreted that the charge is a whole dollar amount. For example, '30025' = $30,025.00 '300.25' = $300.25
Edit Check *Fatal Errors*	• 3901 = Revenue charge is missing • 3903 = Revenue charge is <0 or >Total Charges
Notes	A maximum of 999 revenue codes and corresponding units/charges may be submitted.

Social Security Number

Description	Patient social security number (Inpatient only)
837i Guide	Page 6
UB-04 Element	N/A
HDSS Field	SSN
Format & Valid Codes	Submit social security number with no spaces or dashes.
Edit Check *Fatal Errors*	
Notes	If unknown, put 999999999

Statement Coverage Dates

Description	Dates of the service period included on the bill
837i Guide	Page 7
UB-04 Element	FL 06
HDSS Fields	Statement from Date Statement thru (Discharge) Date
Format & Valid Codes	Dates formatted as specified in the *WVHDDS File Specifications 837i Companion Guide*
Edit Check *Fatal Errors*	• 201 = Discharge date is invalid • 202 = Discharge date is missing • 203 = Discharge date is prior to Admit date (Inpatient only) • 205 = Discharge date is greater than current date • 1101 = Admit date is missing (Inpatient only) • 1102 = Admit date is invalid • 1103 = Admit date is greater than discharge date • 5201 = Statement from date is missing • 5203 = Statement from date is prior to admit date by >3 days (Inpatient only) • 5205 = Statement from date is after statement through date
Notes	The 837 format requires the statement coverage dates to be submitted as one field. They are displayed as two fields in the HDSS.

Total Claim Charges

Description	Total charges billed for the services included on the bill
837i Guide	Page 7
UB-04 Element	N/A
HDSS Field	Total Charges
Format & Valid Codes	Dollar amount – 15-character max (including decimal point). If the decimal point is not submitted, it will be interpreted that the charge is a whole dollar amount.
Edit Check *Fatal Errors*	• 2501 = Total charges revenue code missing • 2508 = Total charges more than +5% of line item total (Inpatient only)
Notes	The charge amount submitted in this field will be presented in the HDSS as the Total Claim Charges (TCHG).

Attachment C

West Virginia Executive Branch
Procedure: Response to Unauthorized Disclosures

Issued by: James L. Pitrolo, Jr.
West Virginia Health Care Authority

1.0 PROCEDURE

This procedure provides the basis of appropriate response to events that may expose personally identifiable information (PII) to unauthorized internal or external persons. It includes procedures for breaches of protected health information (PHI), pursuant to HIPAA.[1] PHI is a subset of PII.

This procedure defines an Unauthorized Disclosure, describes the responsibilities of Executive Branch Department workforce members in connection with Unauthorized Disclosures, and outlines the steps they must take to ensure that Unauthorized Disclosures are properly reported, contained, investigated and mitigated.

2.0 SCOPE

This procedure applies to the Governor's Office and all Departments (including agencies, boards, and commissions) within the Executive Branch of the West Virginia State Government, excluding other constitutional officers, the West Virginia Board of Education, the West Virginia Department of Education, County Boards of Education, and the Public Service Commission.

3.0 REQUIREMENTS

3.1 An Authorized Disclosure is a disclosure of PII to:

3.1.1 Individuals within a Department who have a need to know the PII to conduct Department business;

3.1.2 Third parties who process the PII on a Department's behalf, provided that these third parties have a contractual or legal duty to protect the PII;

3.1.3 Third parties who provide legal, accounting and other advisory services to a Department, provided that these third parties have a contractual or legal duty to protect the PII;

[1] References to HIPAA shall mean the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended by the American Recovery and Reinvestment Act of 2009 (Pub. L. No 111-5) (the "HITECH Act"), any associated regulations and the federal regulations published at 45 CFR parts 160 and 164 (sometimes collectively referred to as "HIPAA").

3.1.4 Other government agencies, for legally required or authorized purposes;

3.1.5 The individual to whom the PII pertains, or the individual who provided the PII to the Department (such as to a member of the workforce who has provided family-member PII for benefits purposes) in accordance with the Individual Rights Policy; and

3.1.6 Any person, if the Department is required by law to make the disclosure (such as in response to FOIA requests) or if the individual to whom the PII pertains consents to the disclosure.

3.2 An Unauthorized Disclosure is any disclosure of PII that is not an Authorized Disclosure; an Unauthorized Disclosure is also known as an incident.

3.2.1 Any known or suspected Unauthorized Disclosures (accidental or otherwise) must be immediately reported in accordance with section 4.0 of this procedure for appropriate investigation and handling

3.2.2 Examples of Unauthorized Disclosures. (List is not exhaustive)

a) Loss or theft of paper records containing PII, such as loss or theft of a briefcase containing papers with PII;

b) Loss or theft of physical information technology (IT) assets including computers, storage devices (such as flash drives), or storage media (such as CDs) that contain PII;

c) Loss or theft of a personal PDA, mobile device or flash drive containing PII;

d) Improper disposal of records, media or equipment containing PII;

e) Accidental or intentional transmission of PII to the wrong person, such as a file being emailed to the wrong recipient;

f) Loss of PII during transit, such as packages that are lost or improperly delivered,

g) Loss of control of PII, such as an inability to locate computers or storage media;

h) Discovery of viruses, spyware or malicious code that intercepts PII;

i) Unauthorized access to systems containing PII; or

j) Transmission of PII to an unauthorized vendor or agency.

4.0 PROCEDURE

4.1 Incident Report. All members of the workforce and contractors (on-site vendors) who access state systems, networks and facilities are to immediately report Unauthorized Disclosures (see section 3.2), on the Office of Technology's (OT) website at https://apps.wv.gov/ot/ir/Default.aspx and to their supervisor and/or manager. If the website is not accessible, the workforce member shall call the OT Service Desk at or 1-877-558-9966. Provide the following information about the incident (or as much as is known):

4.1.1 The date the incident occurred (if known) or was discovered;

4.1.2 The types of PII that were exposed. All actual PII must be redacted or omitted from reports and attachments, including police reports, sent to OT and the State Privacy Office;

4.1.3 How the PII was compromised, including any unauthorized parties that may have accessed the PII;

4.1.4 What steps (if any) have been taken to recover the PII; and

4.1.5 Any other information that may be relevant.

4.2 The State Privacy Office and OT will simultaneously receive the incident report from the website. If notification is made through the OT Service Desk, OT will evaluate whether any PII, including PHI, is impacted by the incident and will notify the State Privacy Office of the same. The State Privacy Office will then notify the appropriate Department Privacy Officer. Additional information may be requested by the State Privacy Office in

order to evaluate the context of the incident report related to the potential, or actual, lost or compromised PII. If the incident report reveals that the Unauthorized Disclosure is most likely a breach, the State Privacy Office will forward the incident report to the Board of Risk and Insurance Management (BRIM).

4.2.1 BRIM will review the incident report and, if appropriate, coordinate with the cyber insurance carrier. BRIM will advise the Department, State Privacy Office and OT as to resources available through the carrier, such as a breach coach, counsel, public relations expertise, call center services, notification assistance, and forensics.

4.3 If the respective Department Privacy Officer first learns of the incident, he or she shall notify OT in accordance with section 4.1.

4.4 For any Unauthorized Disclosure that involves OT systems, the person receiving the report shall notify OT in accordance with OT incident response procedures.

4.5 Once notified of an Unauthorized Disclosure, the Department Privacy Officer shall:

4.5.1 Ensure that OT or other appropriate personnel have been notified so that they can take the steps needed to close any security gaps, such as isolating affected systems, terminating processes that expose PII, etc.

4.5.2 Activate the Department Response Team for their information and action. This Team may provide advice as well as assist in carrying out the Department Privacy Officer's responsibilities under this procedure. This team may be comprised of the Department Privacy Officer, Security Officer, Agency Privacy Officer, Attorney, Communications Director, HR Director, Facilities Manager, business process owner, data owner, and system owner, as needed.

4.5.3 Oversee efforts to recover exposed PII. If PII is recovered, document the basis for any belief that the PII will not be misused

4.5.4 Notify Department leaders, per established procedures. (Notification should include individuals responsible for insurance coverage.)

4.5.5 If the incident may be the result of criminal activity, notify law enforcement or confirm that law enforcement has been notified by OT.

4.5.6 If Payment Card Industry (PCI) data is exposed; notify appropriate financial institutions in accordance with PCI Data Security Standards (DSS). These standards apply to all organizations that store, process or transmit cardholder data – with guidance for software developers and manufacturers of applications and devices used in those transactions. These standards can be found at: https://www.pcisecuritystandards.org/security_standards/index.php.

4.5.7 If PHI is exposed, refer to the Appendix regarding HIPAA obligations. If data elements include those listed in section 4.5.11 of this procedure, then compliance with both HIPAA and W. Va. Code § 46A-2A-101 is required; therefore, follow the remainder of this procedure, as applicable.

4.5.8 Prepare an inventory of exposed data elements.

4.5.9 Using the risk assessment template, analyze possible risks to the affected individuals as a result of the Unauthorized Disclosure. Determine how any risks can be minimized.

4.5.10 If the nature of the incident cannot be fully determined using Department and/or OT resources, contract forensics professionals as needed. See section 4.2.1 regarding resources available through the cyber insurance carrier.

4.5.11 Notify impacted individuals, if required.

a) Follow W. Va. Code § 46A-2A-101, *et seq.*, concerning breach of the security of a computerized system. Good faith acquisition of PII by a member of the workforce is not a breach, provided that the PII was only used for a lawful purpose and not subject to further Unauthorized Disclosure. Impacted individuals must be notified if:

1. The computerized data elements include a West Virginia resident's first name or first initial and last name linked to the individual's

a. Social Security Number;

b. Driver's license or state-issued ID card number; or

c. Financial account number, credit card or debit card number, in combination with any required security code, access code or password; and

2. The data is

a. Unencrypted or unredacted; and

b. Was or is reasonably believed to have been accessed and acquired by an unauthorized person, and

3. The disclosure causes, or it is reasonably believed that it has caused or will cause, identity theft or other fraud

b) Determine whether impacted individuals should otherwise be notified because encrypted data elements are exposed, and are accessed and acquired in an unencrypted form or if they are exposed to an individual with access to the encryption key, and it is believed that the breach has caused or will cause identity theft or other fraud, then notify impacted individuals. For example, a laptop is encrypted, but is lost after the user signs on, the information is now available in unencrypted format and is accessed before the user signs out.

c) The Cabinet Secretary or Agency Head has inherent authority to use discretion to notify in any other situation not otherwise requiring notification.

d) If notification is required, prepare a list of affected individuals. Determine if current contact information for individuals is available to support formal written notification.

Use of last known postal address in the Department's records shall be utilized, if notification is accomplished through mailing. If the Department does not have sufficient contact information, it may notify individuals through substitute notice as defined within W. Va. Code § 46A-2A-101 (7) (D). Notification may also be accomplished via email or telephone. Substitute notice may also be appropriate in certain situations. See *Id.*

e) Note: Individual notification may be delayed if a law enforcement agency advises that notification would impede an investigation or security. Obtain this request in writing for the file.

4.5.12 In consultation with legal counsel, identify applicable laws and determine any risks associated with violations of the laws.

4.5.13 If individual notification is required, consider:

a) Developing a notification plan for Department workforce members and issue a statement reminding them to refer all questions to the Department Privacy Officer;

b) Developing a standby statement for media;

c) Creating a communications outline containing:

1. Basic facts (what happened, what data was exposed, to whom);

2. Steps the Department is taking to mitigate harm;

3. Steps the Department is taking to prevent reoccurrence; and

4. An expression of regret and empathy for the situation.

d) Designating a Department leader who will deliver messages and obtain media training if necessary; and,

e) Creating FAQs to support the communications program.

4.5.14 Where individual notification is required, draft individual notification letters (per security breach notification law):

a) If more than 1,000 individuals must be notified, then the three consumer reporting agencies must also be notified They can be notified at the following websites:

Equifax (800) 525-6285
http://www.equifax.com

Trans Union (800) 680-7289
http://www.transunion.com

Experian (888) 397-3742
http://www.experian.com

b) Determine how questions from affected individuals will be managed. For example, designate an email address, post FAQs on a webpage, take calls at an existing phone number, establish a call center, etc.

c) If a call center is authorized, obtain a toll-free number and train personnel on messages.

d) Print and mail letters when authorized In the few situations when a contracted vendor is visible to the impacted individual(s). Departments may request the vendor take responsibility for notification.

e) Track response, update FAQs, and provide call center training as needed.

4.5.15 Even where individual notification is not required, determine what (if any) individual communications are needed. For example, if members of the workforce are generally aware that "something has happened", it may be prudent to provide a notice to minimize the risks of misinformation/speculation. In these cases, notice may be provided in any manner that makes sense given the situation.

4.5.16 Conduct a post-incident review to determine what steps can be taken to prevent reoccurrence. Document and distribute analysis of the underlying incident and the response to appropriate members

of the Department's leadership team to facilitate organizational learning.

4.5.17 The Department Privacy Officer is responsible for providing a completed Post Incident Report to the State Privacy Office, Chief Technology Officer and Department Cabinet Secretary within 30 calendar days of the Incident Report. All actual PII must be redacted or omitted from this report and any attachments, including police reports, when submitted to OT and the State Privacy Office. If the Post Incident Report reveals that the incident is a breach and that individual notification was required, the State Privacy Office shall forward the Post Incident Report to BRIM.

4.5.18 The Department Privacy Officer may also recommend additional specific controls or improvements to the Privacy Program, including additional training.

5.0 ENFORCEMENT

Any member of the workforce found to have violated this procedure may be subject to disciplinary action up to and including dismissal. Disciplinary action, if determined to be appropriate, will be administered by the employing Department in consultation with the State Privacy Office.

6.0 DEFINITIONS

Refer to Privacy Policy Definitions at http://www.privacy.wv.gov.

Appendix

HIPAA Incident Response

The information contained within this Appendix applies to the West Virginia Executive Branch Procedure: Response to Unauthorized Disclosures.

1.0 BACKGROUND:

A violation of a Department's privacy or security policies or inappropriate use or disclosure of unsecured protected health information (PHI) may result in harm to the person who is the victim of a privacy breach. It may also erode trust in an organization, and impair its ability to provide medical care. It is important to respond quickly to any alleged breach, to determine what occurred, to prevent a recurrence of any violation of policy or law, and to take steps to mitigate any harm. Under HITECH[2], once discovered, an impermissible acquisition, access, use, or disclosure of PHI is presumed to be a breach. Breach notification to the individual (to whom the PHI belongs) as well as to the Secretary of the U.S. Department of Health and Human Services (DHHS), is necessary unless, through a documented HIPAA risk assessment, there is a low probability that the PHI has been compromised. Actual notification processes differ based on the number of individuals affected per breach incident. The timeframe for notification begins when a breach is discovered. Note: A breach is considered "discovered" as of the first day it is known to the covered entity or business associate (BA) (or when by exercising reasonable diligence, the issue would have been known to the organization). Additionally, "known to the covered entity" means when any person (other than the person committing the breach) who is a workforce member or agent of the covered entity is made aware of such breach.

2.0 POLICY:

Based upon breach risk assessment findings, the covered entity Department will determine if unsecured PHI was breached and follow federal and state laws to report such to the affected individual(s). The State Privacy Office will be responsible for reporting such to the Secretary of DHHS. If a Department is a BA (as defined by HIPAA) of a covered entity, the BA Department is responsible for reporting any breach of unsecured PHI immediately to the covered entity, as well as any reporting required under section 4.1 of the main body of the foregoing procedure.

3.0 PROCEDURE:

3.1 Covered Entity Department. The Department Privacy Officer will conduct an immediate review to investigate and determine if the information potentially breached was unsecured PHI, and whether or not individual

[2] Health Information Technology for Economic and Clinical Health Act (HITECH Act), Pub. L. No. 111-5 and any associated regulations published at 45 CFR parts 160 and 164.

breach notification and mitigation must occur. The Omnibus Rule clarified that any potential breach of PHI is subject to the breach risk assessment required process. The steps listed below should be taken in order to accomplish this objective:

3.1.1 Determine whether the PHI was secured. This determination will be made in accordance with the DHHS Guidance document published in the Federal Register on April 27, 2009 which listed and described encryption and destruction as the two technologies and methodologies for rendering PHI unusable, unreadable, or indecipherable to unauthorized individuals. This guidance is currently found at http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/federalregisterbreachrfi.pdf. Note: If the electronic PHI was encrypted according to this Guidance and/or hard copy PHI was appropriately destroyed, individual notification and reporting to the Secretary of DHHS are NOT required. This is known as a "Safe Harbor."

a) If the PHI is considered unsecured, go to Subsection 3.1.2 below.

b) If the PHI was considered secure (in accordance with the above Guidance document and the organization's use of technology), document such in the Department's compliance file and be sure to list what occurred and what steps were taken to address the issue and prevent its reoccurrence. Go to section 3.2.4, below.

3.1.2 Determine whether the unsecured PHI meets the breach exclusions:

a) Unintentional access to PHI in good faith in the course of performing one's job and such access does not result in further impermissible use or disclosure.

b) Inadvertent disclosure of PHI by a person authorized to access PHI at a covered entity or BA to another person authorized to access PHI at the same covered entity, BA or affiliated organized health care arrangement.

c) When PHI is improperly disclosed but the covered entity or BA believes in good faith that the recipient of the unauthorized information would not be able to retain the information.

If the unsecured PHI meets one of the exclusions listed above, document such in the Department's compliance file and be sure to list what occurred and what steps were taken to address the issue and prevent its

reoccurrence. This may include notifying legal counsel as appropriate. If an exclusion is met, go to section 3.2.4, below.

3.1.3 If after review, the PHI was considered unsecured, and no exclusion applies, take the following steps to determine the probability that the security or privacy of the PHI was comprised, and is a breach:

a) Begin with the presumption that the incident is a breach, unless the covered entity or BA, as applicable, demonstrates that there is a low probability that the PHI has been compromised. Assess the level (low, medium or high) of probability that the PHI was "compromised," based on a risk assessment of at least the following factors:

1. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification,

2. The unauthorized person who used the PHI or to whom the disclosure was made;

3. Whether the PHI was actually acquired or viewed; and

4 The extent to which the risk to the PHI has been mitigated.

If there is a medium or high probability that the PHI is "compromised," go to subsection 3.1.4, below. If there is a low probability that the PHI is "compromised", document such in your Department's compliance file, be sure to list what occurred and what steps were taken to address the issue and prevent its reoccurrence. Go to section 4.0 in the foregoing procedure.

3.1.4 Based on the analysis and resulting findings performed above, the Department Privacy Officer will develop a plan to mitigate the harm, to the extent that this is practicable, and will document the extent to which the risk to the PHI has been mitigated and any other reasonable factors related to the incident. Also follow sections 4.5.8 through 4.5.16 in the foregoing procedure. Document a final conclusion based on whether or not the final probability that the PHI has been compromised is low, medium or high. If applicable, evaluate what actions the Department requests the BA to take, including covering costs, in accordance with the Business Associate Agreement.

3.1.5 The Department Privacy Officer will notify each affected individual(s) whose information has been inappropriately accessed,

acquired or disclosed during such breach. If such breach was caused by a BA, it may be, based on the language within the Business Associate Agreement, the BA's responsibility to perform the following notification steps and to inform the covered entity of such.

a) Using the breach notification log, list the identification of each individual whose unsecured PHI has been, or is reasonably believed to have been accessed, acquired or disclosed during such breach.

b) Once information has been validated, prepare to notify each individual as soon as possible, but within 60 calendar days from discovering the breach. NOTE: All notification materials should be organized and maintained, as the ability for the Department to demonstrate its attempts at notification is an American Recovery and Reinvestment Act of 2009 (ARRA) requirement.

3.1.6 Notification Steps to be followed:

a) Individual Notice Affecting 499 or Fewer Individuals

1 Individual notice must be provided via first class mail at the last known address or email if preferred by the individual (which may have been recorded on the Notice of Privacy Practices Acknowledgement (or other) form).

2. If the individual is deceased, the notice must be sent to the last known address of the next of kin, or personal representative. The Department is only required to provide notice to the next of kin or personal representative, if it is known that the individual is deceased and has the address of the next of kin or personal representative.

3. If there are 10 or fewer individuals for whom the Department has insufficient or out-of-date contact information to provide the written notice, the Department is permitted to provide notice to such individuals through an alternative form of written notice, by telephone or other means, e.g., email, even if the patient has not agreed to electronic notice.

4. If there are 10 or more individuals for whom insufficient or out of date contact information exists, the Department must provide a substitute notice by posting the notice for a period of 90 calendar days on

Attachment D

West Virginia Health Care Authority

Information Security and Privacy Policy

Version 2.0

Issued By: Health Care Authority Board

Policy No: WVHCA-1001 **Issue Date:** June 15, 2016 **Effective Date:** July 1, 2016

Acknowledgements

The following individuals contributed to drafting, reviewing, or providing input for this policy: Tim Adkins, Laura Anderson, Terri Barrett, Shelley Baston, Neil Brown, Donna Crane, Sam Curia, Cynthia Dellinger, Susan Dolly, Mary Fitzgerald, John Grey, Sue Haga, Denise Hershey, Sharon Hill, Paula Marshall, Jennifer Meeks, Sallie Milam, Kristi Pritt, Victor Richardson, Barbara Skeen, Lori Tarr, and members of the West Virginia Executive Branch Privacy Management Team.

Table of Contents

1.0 INTRODUCTION

This document provides policies, standards, and rules for the use and protection of the information, information technology, and security assets owned or maintained by the West Virginia Health Care Authority (HCA).[1] This policy applies to the Board and all members of the HCA workforce, including West Virginia Health Information Network (WVHIN) employees (all known as users). All users are required to read, agree to, and sign this policy. Users who violate this policy may receive progressive discipline, up to and including dismissal. This policy supersedes existing acceptable use, privacy and security policies. The West Virginia Health Care Authority expressly reserves the right to change, modify, and/or delete this policy at any time.

The Following Section Applies to All Users

2.0 USER RESPONSIBILITIES

All users are responsible for protecting HCA's information and information systems, such as computers, phones, laptops, tablets and networks.

2.1 Confidentiality Agreement

All users shall sign a confidentiality agreement upon hire and annually thereafter.

2.2 Information Classification and Inventory

HCA shall keep an inventory of all data it holds, including personally identifiable information. HCA shall classify all data by level of sensitivity. Users who receive or create data not already classified or inventoried by HCA must notify their Department Director (DD) and the Information Security Officer (ISO).

Restricted Information: Any information which both identifies an individual and contains other information about that individual whose disclosure is prohibited or limited by law. Often thought of as private information; if unauthorized persons accessed these data, it could cause financial loss or identity theft. Restricted information is only made available to authorized users who "need to know" such information. Examples include Social Security numbers, driver's license numbers, and individually identifiable health information, such as hospital discharge data.

Sensitive Information: These are the majority of data and includes any information which is not categorized as restricted, and is made available through formal record requests or requests for disclosure. Sensitive information is only made available to authorized users who "need to

[1] See Appendix A for National Institute of Standards and Technology (NIST) and Health Insurance Portability and Accountability Act (HIPAA) references.

know" such information. Examples include driver history records, personal email addresses, training program data, and certain health care survey data.

Public Information: Public data with no distribution limitations. One example is publicly released data de-identified pursuant to this policy.

2.3 Sensitive and Restricted Information Safeguards

Users may not take sensitive or restricted information off HCA's premises or systems. Such information may only be disclosed pursuant to the provisions of this policy. Such information shall not be posted, displayed, or stored in any area of the facility regularly accessible by users, visitors, or other third parties. Documents containing sensitive or restricted information must be shredded as soon as no longer needed, per HCA's record retention policies. Digital files must be permanently deleted.

Special Safeguards – Applied Only to Restricted Information

If possible, users shall make sure that any form, document, or application that contains restricted information has a conspicuous warning of that fact. Users may only process such information when they have a "need to know." Users shall only access the minimum amount of restricted information needed to perform their HCA defined duties. Protected Health Information (PHI) as defined and protected by HIPAA[2] may not be used or disclosed in any form except by members of the WVHIN, State Privacy Office and the IT Division, in compliance with procedure. Any other user who receives PHI shall immediately contact the Privacy Officer to determine whether to destroy or redact it.

Users shall take reasonable measures to secure the use of restricted information in their personal workspace. Device screens should not be viewable without a user's knowledge. Users must lock or logoff of devices before leaving them unattended. Paper documents should be stored in a locked area. Restricted information should only be discussed in private. Users should collect any restricted information they print at once. Users should not leave devices printing such information alone.

Faxes must include a cover sheet with a confidentiality warning. Users should confirm a fax was sent to the right number and collect the original. Mail must be sent in a sealed envelope with a confidentiality warning. Mail must be sent with tracking. Users shall access and use non-HCA systems in compliance with their respective security and privacy rules. For all other restricted information, users may only send restricted digital information through an HCA service, such as a secure HCA portal. When given an option, users shall allow the system to generate the password. Any other transmission shall be approved in writing by the ISO and shall be encrypted. When possible, users should ask that restricted information be sent to them using these rules.

[2] HIPAA – the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended by the American Recovery and Reinvestment Act of 2009 (Pub. L. No. 111-5) (the "HITECH Act"), and any associated regulations and the federal regulations published at 45 CFR parts 160 and 164 (sometimes collectively referred to as "HIPAA").

2.4 Information System Access[3]

Access to any HCA information system is granted according to the principles of "need to know" and "minimum necessary." A request for access must be approved by a user's DD and sent to the ISO. Users must protect their passwords. Passwords may only be recorded using a HCA approved tool. Users may only work with HCA information using an HCA approved information system.

2.5 HCA Computing Devices

Users must limit personal use of HCA devices to a reasonable and limited amount. Personal use of HCA devices may not violate HCA policy, or law. Users should not use their personal email address for HCA's business. Users may not stream or download non-HCA business related media such as videos, music, or games without the ISO's approval. Users may not put personal security protections on HCA devices without the ISO's written approval. It is recommended that users store information created for HCA's business or on behalf of HCA on HCA's servers. Non-HCA business information may not be stored on HCA's file servers. Users must contact the ISO when an HCA device needs repair or support. Users may connect to the HCA secure wireless network, but should not connect to HCA's guest unsecured wireless network. Users who want to move or dispose of any hardware must submit a written request to the ISO. Users may not modify any HCA information system or device without the ISO's written approval. Users must submit all change requests using the change request form.

2.6 Personal Computing Devices

Users may use personal devices for HCA business. Users must ensure that HCA data cannot be seen or accessed by a third party. Users must use HCA's password rules on their device. Users must keep their device current with the latest security updates. The use of any device which has had its native operating system changed, or undermined in any way not intended by the manufacturer, is strictly prohibited. For security, users should not connect their device to HCA's less secure guest wireless network. The loss of any device must be reported as an incident.

Users must remove all HCA resources and log-on credentials from their device prior to replacing, upgrading, selling, or giving up possession of the device in any manner. If a user is not able to remove HCA resources and log-on credentials they must contact the ISO. Users may not download and save any HCA electronic files to their device that may contain restricted information.

HCA respects the privacy of personal devices and will only request access to those devices to implement security controls or to respond to legal processes. Users may contact the HCA IT department seeking repairs or support services for their personal devices, but such repair or support shall occur at HCA's discretion.

[3] This policy does not govern information systems controlled and maintained exclusively by the West Virginia Health Information Network as defined in W. Va. Code § 16-29G-1 *et seq.* and W.Va. CSR § 65-28-1 *et seq.*

The addition of HCA software may decrease the available memory or storage available on a device. Business use may cause an increase in personal service plan costs. HCA will not reimburse users for the cost of the device, its maintenance and repair, or its service plan. Use of personal devices for HCA business activities is strictly voluntary and neither prescribed nor encouraged. HCA is not responsible for any loss or theft of, damage to, or failure of personal devices that may result from use for HCA business. Contacting vendors for trouble-shooting and support of third-party software is the user's responsibility.

A. Personal Mobile Devices – Specific Requirements

Mobile device refers to portable devices, such as cell phones and media tablets (e.g. Apple iPads). Laptop computers are not covered by this section. Users may access their HCA email, calendar, contacts, and remote desktop with HCA approved applications, such as through the HCA portal. HCA has a zero-tolerance policy for texting or emailing while driving. Only hands-free talking while driving is permitted.

B. Personal Computers – Specific Requirements

Users may use their personal computer from an alternate location to access their remote desktop with an HCA approved application. Users may also access HCA web resources like remote mail. Users must use a secure wired network, or a password protected wireless network. Users must maintain up-to-date HCA approved anti-virus software on their device.

In some cases, users may also use their personal computer on the internal HCA network. Users must first turn over their device to the HCA IT department for inspection, approval, set-up, and registration.

C. Public Computers – Specific Requirements

Users are discouraged from using any computer they do not own to access HCA resources or perform HCA business activities. Users who cannot avoid using a public computer must notify the ISO in writing. The notice must include the time, place, and nature of the access.

2.7 Network Security

Users may not connect new devices to or modify the HCA network without the ISO's written approval. Users may access certain HCA information systems from home if a business need exists such as participation in the alternate work site program. Users may not remotely access restricted information, unless utilizing HCA equipment and with the ISO's written approval. To obtain remote access, users must submit a request under the Information System Access section (2.4) of this policy.

2.8 Incident Reporting and Response

Users shall report violations or suspected violations of this policy as well as any other suspicious or irregular activity as soon as possible. Security or privacy incidents must be reported to a user's immediate manager and through the incident reporting form. After hours incidents must be reported by calling the ISO; users must also report the incident when they return to work.

2.9 User Information Privacy and Ownership

HCA respects the privacy of users, however, users shall have no expectation of privacy in their use of any HCA information, information technology, or security assets. In its support and maintenance of its information systems and technologies, HCA will generally avoid accessing, reviewing, using, disclosing or retaining user's personal information. In certain circumstances, however, the access, review, use, disclosure, or retention of personal information may be necessary. All materials, data communications and information created for HCA business or on behalf of HCA, including but not limited to email (both outgoing and incoming), telephone conversations and voice mail recordings, instant messages, and internet and social media posting and activities ("content") are the property of HCA.

In order to prevent misuse, HCA reserves the right to monitor, intercept, review and erase, without further notice, all content created on, transmitted to, received or printed from, or stored or recorded on HCA equipment, or if on personal equipment, created for HCA business or on behalf of HCA. HCA may also store copies of such content for a period of time after it is created, and may delete such copies from time to time without notice. In addition, HCA may obtain and disclose copies of such content, including personal content, for litigation, investigations, and auditing purposes. All network traffic shall be subject to electronic monitoring.

2.10 Physical Security

Users shall only access HCA facilities using their approved key, access card or access code, and may not share or loan their HCA facility key, access card or code to another individual. Outside of normal business hours, users may not access HCA facilities for any non-HCA purpose. Users must require that any visitor they invite to HCA's facilities sign in as a guest. Users are responsible for the actions of any visitor they bring to HCA's facilities after normal business hours. Users must accompany afterhours visitors at all times. Users shall sign in any after-hours visitors when they return to work during business hours. Users should immediately report any suspicious visitors to the Executive Director.

2.11 Training and Awareness

Each new user must complete the following training courses through the West Virginia Office of Technology's Learning Management System (LMS) upon hire: Confidentiality Agreement, Privacy Awareness, HIPAA/HITECH training, and Cyber Security Awareness Training. In addition, each new user will be trained on the HCA Information Security and Privacy Policy.

The following training and privacy awareness will be provided to all users:

- Annual Confidentiality Agreement execution (Review Policy and Sign)
- Biannual Privacy & Annual Cyber Security Awareness training
- Periodic privacy and security awareness tips
- Revisions and/or material changes to the HCA Information Security and Privacy Policy as they occur.

2.12 Data Disclosure

Users may not disclose any sensitive or restricted data to a third party except as allowed in this section. Sensitive and restricted data not included within HCA data sets, such as certain human resource and fiscal data, shall only be used or disclosed where they are reasonably needed by the third party to accomplish the legitimate business purpose of the use or disclosure. Data sets covered by this section include Hospital Uniform Billing data, Financial Disclosure data, survey data, Healthcare Associated Infection data, All Payer Claims Database and other data.
HIPAA regulated data disclosure for WVHIN and the State Privacy Office is not covered by this policy and shall be delineated in division procedure.

A. Data Disclosure Generally

HCA operates under a strict directive to "maintain the confidentiality of any and all medical or individual information personally identifiable to a patient or a consumer of health services, whether directly or indirectly." 65 W.Va. CSR § 9.1. To that end, the provisions of this policy are to be strictly construed in favor of maintaining that confidentiality unless so doing would violate clearly established law. HCA reserves the right not to provide any or all of the data requested in its sole discretion and not to provide any or all data requested by parties that have previously violated the terms of a data use agreement or otherwise misused any of HCA's data.

The HCA shall establish a Privacy Committee for the purpose of assisting in decisions regarding maintaining patient confidentiality. The Privacy Committee's membership shall be flexible to address relevant issues, but shall generally consist of the following:

- Privacy Division,
- Information Security Officer, and
- Division Directors and Supervisors of data-related divisions.

The Privacy Committee shall be chaired by the Privacy Officer.

Users shall verify the identity and authority of the data requestor prior to disclosure. If the identity and authority is already known to the user, then no further action is required. If not, then this may be confirmed by having the request submitted on agency letterhead or through the submission of credentials. Authorization is confirmed through the agency's execution of a Data Use Agreement.

A provider submitting data may directly obtain the full set of data, except for tax returns, that it has submitted without statistical disclosure limitation techniques, including cell size limitation or suppression. HCA may limit this data to such data for which it is the direct custodian. HCA reserves the right to pass along any data retrieval costs to the requestor. Each Division shall adopt procedures to ensure that controls are established consistent with the sensitivity of the data to be transmitted.

The use and disclosure of direct and certain indirect identifiers ("confidential identifiers"), such as a Social Security number or street address, which are derived from a single individual, pose a high risk that the identity of that individual may be ascertained. Accordingly, the use

and disclosure of the following patient confidential identifiers is strictly prohibited unless the HCA has approved such a use or disclosure, or law requires it: name, home street address, home telephone number, home fax number, personal electronic mail address, Social Security number, certificate number, license number, vehicle identifier number, license plate number, device identifier and serial number, personal web universal resource locator (URL), internet protocol address number, biometric identifier, and full face photographic images and any comparable images.

B. De-identification

De-identification is the process by which direct, and certain indirect identifiers are removed from data derived directly from an individual and the data are manipulated to reduce the risk of the individuals' re-identification.

1. Definitions

Sensitive or identifying variables are those variables that directly or indirectly identify or track a particular individual (e.g. variables which describe an individual such as demographic information, sex, dates, or locations). **Non-sensitive or descriptive variables** are those variables that exist to identify or track actions taken or determinations made by the data collector (e.g. variables which describe something that happened to an individual or during an event). Taken alone, these variables have little to no potential for identifying the individual.

Data aggregation is any process in which information composed of records or variables is expressed in a high-level summary form for purposes such as reporting or analysis. **Suppression** occurs when variables that may render a record personally identifiable are removed from the dataset. **Generalization** occurs when variables that may render a record personally identifiable are rendered less precise through categorization. **Minimum cell-size** is the minimum quantity of identically unique variable combinations that may be present in a de-identified dataset.

2. De-identification Procedures

No disclosure shall be made consisting of more variables than are requested or needed for the stated purpose of a request (e.g. every variable is necessary and the data are not available from other sources). However, publically released data and precompiled reports or datasets may be disclosed, even when they contain more than the minimum data necessary.

a. Record Level Data

Publicly released data are data that are made accessible indiscriminately through some public medium (e.g. the internet). Such data are subject to strict de-identification requirements. Publically released data sets shall be de-identified utilizing the following techniques: There shall be a minimum of 10 records for every sensitive variable in the dataset. This may be accomplished through aggregating geography or years accordingly.

Additionally, the following patient variables must be omitted:

1. Names;
2. Specific geographies:
    a. Street address,
    b. city,
    c. county with a population below 10,000,
    d. precinct,
    e. zip code, except:
        i. for the initial three digits of a zip code if according to the current publicly available data from the Bureau of Census: the initial geographic unit formed by combining all zip codes with the same three initial digits that contain more than 10,000 and;
        ii. the initial three digits of a zip code for all such geographic units containing 10,000 or fewer is aggregated with a geographic unit equal to or greater than 10,000; and
    f. equivalent geocodes, (longitude and latitude)
3. All elements of dates (except year) for dates directly related to an individual, including dates of service, birth date, date of death, and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of 90 or older;
4. Telephone numbers;
5. Fax numbers;
6. Electronic mail addresses;
7. Social security numbers;
8. Medical record numbers;
9. Health plan beneficiary numbers;
10. Account numbers;
11. Certificate/license numbers;
12. Vehicle identifiers and serial numbers, including license plate numbers;
13. Device identifiers and serial numbers;
14. Web Universal Resource Locators (URLs);
15. Internet Protocol (IP) address numbers;
16. Biometric identifiers, including finger and voice prints;
17. Full face photographic images and any comparable images; and
18. Any other unique identifying number, characteristic, or code.

Further, discharge year and admission year shall not be disclosed for the same record. Where patient county or region and state of residence are included, then length of stay is not included for the same record.

Public use files are precompiled reports or datasets which are made available for any appropriate purpose provided the party first executes a data use agreement with HCA. Public use files shall have a minimum cell-size of 5 for every **sensitive variable** present in the data set.

Existing aggregated files shall be sorted by discharges, length of stay, total charges and DRG or MSDRG case weight. These aggregated files contain patient year of discharge, patient age range, and patient county of residence.

Custom data requests are any third party requests for HCA to generate reports or datasets that it does not regularly make available through public release or public use files. Generally, no disclosure shall be made, unless a stated purpose for the disclosure has been provided which is consistent with HCA's mission and memorialized in the data use agreement. Generally, users may only disclose custom datasets which are appropriately de-identified, under a data use agreement, and if applicable, in compliance with subsection E, Use and Disclosure of Confidential Identifiers. Generally reports or datasets generated pursuant to custom data requests shall have a minimum cell-size of 5 for every **sensitive variable** present in the data set. In the unusual circumstance, when an individual or organization is granted continuing and ongoing access to data, this arrangement is governed separately by a Memoranda of Understanding.

b. Survey Data

Publicly released data must be appropriately de-identified such that no user is able to correctly align the disparate data features (variables) into a record that contains sex, date of birth (or year of birth) or zip code (or county) relative to a single patient. For confidentiality of date or year of birth, generally age ranges shall be used. With race and ethnicity, and special populations (such as developmental disability status and veteran status) , the HCA Privacy Committee shall review these data variables to determine inclusion, particularly where a county has low numbers of a certain race or ethnicity. After the survey data are received and prior to disclosure, the HCA Privacy Committee shall review the data, changes in law, technology or best practice. Agencies that serve only one county shall receive an enhanced review. All e-mail addresses, home addresses, geolocation data, and, generally, open comments fields shall be suppressed.

Public use files
Execution of a data use agreement shall be required of the recipient of a public use file. In addition to non-sensitive data, this file may contain the following data varibles not available within publicly released data: age <1, ethnicity, race, developmental disability status, veteran status and specific codes. Additionally, where a respondent's survey results have been suppressed, and there are between 5 and 10 patients, these data may be made available in a public use file. Generally, open comment fields shall not be made available in a public use file.

C. Special Rules for APCD, HAI and Other Data

All-Payer Claims Database (APCD) data are any data collected for and stored in the APCD pursuant to W.Va. Code § 33-4A-2. Pursuant to 114A CSR § 2-4.3, APCD data may not be disclosed to anyone except, where the completeness and quality review indicates a problem with the data, to Memorandum of Understanding (MOU) parties (Chairperson of HCA, West Virginia Insurance Commissioner, and Secretary of the West Virginia Department of Health and Human Services) and the data submitter when such disclosure is required to facilitate the data collection process.

HAI data are healthcare-associated infection data collected pursuant to W. Va. Code § 16-5B-17. Pursuant to 64 CSR § 7-9, HCA is required to allow Bureau for Public Health access to the National Healthcare Safety Network (NHSN) data. Upon receipt of a request for data or a

report from any organization or individual other than the Bureau for Public Health, the Healthcare Associated Infection Advisory Panel shall review and recommend to the HCA whether and how the request might be granted. HAI data are confidential and may only be reported publicly in the aggregate and de-identified to the standards for the public release of record level data found above in section 2.12.B.2.a. Should the Panel recommend that HAI data be shared with an organization, the data shall be de-identified to the standards regarding the release of a custom record level data request found above in the same section. The Panel shall recommend any additional safeguards necessary to benefit the public's understanding, the privacy and security of the data, as well as the HAI data reporting program.

Other data are data residing in the HCA's data warehouse that has been obtained from other state agencies, private organizations, or any other source not referenced herein and not including data received pursuant to W. Va. Code § 16-5F-1 or W. Va. C.S.R. 65-13. The HCA will evaluate requests for these data on a case by case basis and will generally only disclose such data in a de-identified data set pursuant to subsection B above when a compelling state interest is set forth to justify such a disclosure or by consent of the data owner. Generally, the HCA shall require the data requestor to execute a data use agreement. Finally, the HCA's right to disclose these data may be restricted by contractual terms and the HCA may be unable to provide the requested data.

D. Specific Types of Requests

A request made for certificate of need (CON) data or information is a request made by or on behalf of a healthcare provider or healthcare facility covered under W.Va. Code § 16-2D-1 *et seq.* or W.Va. Code § 16-29B-19 for the purpose of planning or evaluating future activities which may implicate the CON process. Because precise calculations are key to the CON process, minimum cell-size requirements and other controls, such as removal of unique records, may not be applied to data disclosed to covered facilities for CON. Such disclosures, however, still require a signed data use agreement. Further CON files may contain limited indirect identifiers, such as a patient account number, where determined to be legally necessary.

A Freedom of Information Act (FOIA) request is any request for data or information held by HCA made pursuant to the West Virginia Freedom of Information Act (W.Va. Code § 29B-1-1). Any FOIA request or subpoena received by HCA shall be submitted to HCA's General Counsel for a review and determination of how, if at all, the request may be fulfilled.

A news media request is any non-FOIA data request made for journalistic rather than scientific purposes. All non-FOIA data requests made for journalistic purposes shall be submitted to the HCA Board Chairperson. The HCA Board Chairperson may elect to serve as an intermediary for the request or return the request to the appropriate department for fulfillment.

E. Use and Disclosure of Confidential Identifiers

All requests for the use and disclosure of confidential identifiers[4] shall be reviewed by the HCA Privacy Committee. The Privacy Committee shall make recommendations to the HCA

[4] Defined previously in 2.12.A

Chair and Executive Director regarding the approval of the use and disclosure of confidential identifiers upon the request of any user or third party.

The HCA shall never access, use or disclose confidential identifiers in plaintext. Confidential identifiers shall be field-level encrypted using industry best practice FIPS 140-2 approved encryption algorithms, with the encryption keys maintained on a separate device and not accessible in plaintext by HCA staff.

The HCA shall only approve a request for the use or disclosure of encrypted confidential identifiers based on its determination that the use or disclosure involves no more than minimal risk to the privacy of individuals based on at least the presence of:

(1) An appropriate plan to protect identifiers from improper use and disclosure, including compliance with federal substance abuse regulations found in 42 CFR Part 2;
(2) An appropriate plan to destroy those identifiers at the earliest opportunity, consistent with the intended use, unless the requestor plans to return the identifiers. If the data are destroyed, the requestor must submit the following: the date of the destruction, the means used to destroy the data, and two people within the organization must certify that the destruction actually took place;
(3) Written assurances that the identifiers will not be reused or disclosed to any other person or entity except
(a) As required by law,
(b) For authorized oversight of the intended use, or
(c) For other purposes for which the use or disclosure of the identifiers is permitted by this policy; and
(4) A compelling purpose, in line with HCA's statutory purpose, that protects the health and well-being of West Virginians by guarding against unreasonable loss of economic resources or ensures the continuation of appropriate access to cost-effective, high-quality health care services as specified.

Before data may be released, HCA must document and record the members of the approving Privacy Committee, the date of the recommendation for approval, a statement that the HCA Privacy Committee has determined that all of the specified criteria for an approval were met, a brief description of the identifiers for which use or access has been determined by the Privacy Committee to be necessary in connection with the intended use, and the signature of the HCA Privacy Committee chair.

The Following Sections Apply to HCA Administrators Only

Every user is essential to the protection of HCA information and information systems. However, some management-level users have specific responsibilities identified in this section.

3.0 ADMINISTRATIVE ROLES

TITLE	ROLES
Executive Director (**XD**)	• Responsible for oversight of the security and privacy programs; primarily responsible for physical security.
Information Security Officer (**ISO**)	• Responsible for the management, promotion and protection of HCA's information security.
Privacy Officer (**PO**)	• Responsible for the management, promotion and privacy of HCA's PII (including PHI).
Human Resources Director (**HRD**)	• Responsible for providing access to HCA's offices; maintains documentation of employee privacy and security training and compliance; coordinates with the **ISO** in de-provisioning employees.
Chief Financial Officer (**CFO**)	• Responsible for the acquisition and maintenance of HCA's physical asset and financial inventory and for ensuring that purchases comply with this policy.
WVHIN Procurement Officer (**WPO**)	• Responsible for ensuring that purchases comply with this policy.
Department Director & Supervisor (**DD/S**)	• Responsible for ensuring their departments create and implement the controls and procedures required by this policy.

4.0 ADMINISTRATIVE, TECHNICAL & PHYSICAL CONTROLS

CONTROL	RESPONSIBILITY
4.1 Confidentiality Agreement	• **PO** Ensures that HCA utilizes the Executive Branch Confidentiality Agreement, and maintains documentation of the same. • **HRD** Works with **PO** to ensure all users complete the Confidentiality Agreement.**DD/S** Sets performance standards for their employees, ensuring that all comply with the Confidentiality Agreement and all other HCA policies and procedures.
4.2 Information Classification and Inventory	• **ISO** Maintains the HCA information inventory. • **PO** Conducts periodic audits of the HCA information inventory. • **DD/S** Conducts an annual inventory of all information held by his/her department including its classification and location and reports such to the **ISO**.

4.3 Sensitive & Restricted Information Safeguards	• **ISO** Ensures that all printers, photocopiers, and fax machines are inaccessible to visitors and other third parties. Designates NIST approved methods for encrypting restricted information. Maintains written procedure for encryption methods. Ensures that confidential identifiers in HCA information systems are masked. Configures and ensures fax machines, printers and copiers are encrypted or employ immediate memory overwriting. To the extent practicable, reviews non-HCA systems processing HCA information and encourages the system owner to have appropriate terms and conditions. • **PO** Conducts periodic audits to determine whether documents containing sensitive or restricted information are shredded as soon as no longer needed, per HCA's record retention policies. Also audits whether digital files are permanently deleted. • **CFO** Reviews all HCA purchasing requests for printers or faxes to ensure that the devices have been approved by the **ISO**. • **WPO** Reviews all WVHIN purchasing requests for printers or faxes to ensure that the devices have been approved by the **ISO**. • **DD/S** For restricted information: Ensures that physical documents containing restricted information are stored in a secure container or area. Ensures the tools used by his/her department display a conspicuous warning that the information is restricted. Approves any alteration of information stored in HCA systems. Maintains documentation of all alterations.
4.4 Information System Access	• **ISO** Stores and maintains user access profiles. Makes profiles available to all relevant parties on request. Ensures users are granted access only to necessary systems. Retrieves HCA devices and security assets from users leaving HCA employ, and ensures their access is revoked. (Disabled accounts shall be maintained for 60 days prior to deletion.) Maintains an inventory of all users, software programs, and other systems that access HCA information systems. Periodically reconciles system access inventories with access logs. Ensures third parties have executed MOUs or contracts before granting access. Ensures all users have a unique username. Creates password standards and requirements. Disables accounts after three failed log-in attempts. Requires that passwords be changed after 60 days or account will be disabled. Enables security banner for access to all systems. • **PO** Periodically reviews access profiles for accuracy and policy violations. • **HRD** Ensures users have received required training within 30 days of change in access. Notifies **ISO** of any new users or change in user's employment status. • **DD/S** Reviews and submits access profiles and modifications to profiles for his/her employees to the **ISO**.

4.5 HCA Computing Devices	• **ISO** Limits configuration changes by users. Limits user installation or execution of software. Ensures all devices are equipped with antivirus software. Tests software and firmware for effectiveness and side effects prior to installation.
4.6 Personal Computing Devices	• **ISO** Approves all user access to HCA owned and maintained computer systems. Approves all anti-virus software. Completes an initial inspection, set-up, registration and determines if the personal computer is suitable for use on HCA premises. Upon user's request, **ISO** removes all HCA resources and login credentials prior to the user replacing, upgrading, selling or giving up possession of the device in any manner as well as when users seek third party repair or support. In the event of a damaged, lost or stolen device, thereby preventing removal of HCA resources and login credentials, the **ISO** should attempt to reset the device upon the user's request. Resets login credentials when they are notified when users access HCA resources from public computers. May provide HCA repairs or support services for personal devices.
4.7 Network Security	• **ISO** Periodically audits remote access log for suspicious activity. Documents all devices and applications connected to the internal HCA network, including interface characteristics, security requirements, and the classification of the data communicated. Grants third-party remote access only to pre-documented devices and network addresses. Reports any significant virus detection as a security incident. Ensures that firewalls and intrusion detection are enabled and effective. Hides internal network addresses from external view. Monitors and logs all remote access to HCA information systems. Ensures physical security of network resources.
4.8 Incident Reporting and Response	• **ISO** Maintains secure incident reporting tool which automatically reports to WV Office of Technology's tool. • **PO** Develops content for incident reporting tool with **ISO**. Maintains six-year log of all reported incidents, including post incident reports. • **ISO** & **PO** Conduct incident investigations, engage HCA Privacy Committee as appropriate, and report findings to **XD** where appropriate.
4.9 User Information Privacy and Ownership	• **ISO** Will avoid accessing, reviewing, using, disclosing or retaining users' personal information, except when infeasible.
4.10 Physical Security	• **XD** Responsible for all physical security of HCA facilities. Ensures that only authorized and logged individuals gain access to HCA's facilities during normal business hours. Notifies the **ISO** of any service, sale, or disposal of physical security assets. • **ISO** Ensures that non-public printers, copiers and fax machines will not be located in areas frequented by the public. • **HRD** Provides and maintains security system, user facility keys, access cards, codes and master keys to HCA facilities.

4.11 Training and Awareness	• **ISO** and **PO** Delivers Privacy Awareness training every two years and Cyber Security Awareness training annually. • **PO** Delivers initial security and privacy policy training at on-boarding, and additional training when policy changes occur. Maintains documentation of privacy and security training. • **HRD** Works with **ISO** and **PO** to ensure all users complete training.
4.12 Data Disclosure	• **ISO** Serves on the HCA Privacy Committee. • **PO** Convenes and chairs the HCA Privacy Committee. • **DD/S** Coordinates with **PO** to implement procedures for the documentation and review of all disclosures of sensitive and restricted information outside of HCA. Those **DD/S** who manage data-related divisions also serve on the HCA Privacy Committee and may request that the board meet to address data privacy issues.
4.13Asset Inventory	• **ISO** Ensures that all software is used in accordance with contracts and laws and maintains inventory of all information technology assets, including physical hardware and software assets. • **CFO** Tags all information technology assets in compliance with State rules and maintains and stores documentation. Works with **ISO** to maintain inventory, including the date of acquisition, type, user, location, and uniquely identifying identification number of all tagged assets.
4.14 Change Control	• **ISO** Reviews all access and network configuration change requests with relevant parties. Ensures all change requests are properly documented and implemented. Maintains secure change request form and log of all changes.
4.15 Contingency Planning	• **XD** Identifies HCA's essential mission and business functions to be preserved following an information system disruption, compromise, or failure. • **ISO** Ensures that all mission-essential HCA information and information systems are regularly backed up both locally and at an off-site location. Conducts annual training, testing and review and updates the plan accordingly. Develops and disseminates plan to continue HCA's essential mission and business functions in the event of an information system disruption, compromise or failure, and to recover all HCA information and information systems. Establishes backup retention schedule and ensures that all HCA information and information services are backed up and retained according to the schedule.
4.16Acquisition, Maintenance, Sale, Movement or Disposal of Hardware	• **ISO** Obtains, protects, and makes available all information system documentation as needed. Ensures that "mirror images" of appropriate devices are created before off-site service, sale or movement, and that all data are permanently erased. Obtains approval from WV Office of Surplus Property and WV Office of Technology before retiring devices.

4.16Acquisition, Maintenance, Sale, Movement or Disposal of Hardware (continued)	• **CFO/WPO** Obtains information security specifications from the **ISO** prior to the acquisition of any information systems or information system services.
4.17 Security Risk Assessments	• **XD** reports significant security risk assessment results to the HCA board. • **ISO** Conducts periodic assessments of risk, sends results to the **PO** and **XD**. Periodically scans information systems and hosted applications for vulnerabilities, and documents, reviews, remediates such and reports to the **XD**. Ensures that any new security or privacy risks are mitigated. • **PO** Supports the **ISO** in conducting and reviewing vulnerabilities, risk assessments and mitigation execution.
4.18 Privacy Impact Assessments (PIA)	• **PO** Assists with completing PIAs and coordinates with **ISO** as needed. Maintains records of PIAs. • **CFO/WPO** Reviews contracts with privacy impact to determine PIA completion and proper terms in contract. • **DD/S** Completes a PIA prior to starting any new activity which might affect the security or privacy of HCA information or information systems. Notifies **CFO** of potential contracts with privacy impact.
4.19 Audit & Accountability	• **ISO** Determines which information system events will be audited. Periodically reviews and analyzes audit logs for unusual activity. Provides audit report to **XD** as appropriate. Maintains audit records for specified retention period. Implements an automated process to notify **ISO** of any audit processing failure by the system.

APPENDIX A

Privacy Crosswalk between HCA Information Security and Privacy Policy and NIST Special Publications & HIPAA (45 CFR § 164)

	Section	Reference
1.0	**Introduction**	NIST 800-53 Appx. F: PS-1, PS-8
2.0	**User Responsibilities**	NIST 800-53 Appx. F: PS-1 NIST 800-53 Appx. J: AR-1(d)
	2.1 Confidentiality Agreement	NIST 800-53 Appx. F: PL-4, PS-6 NIST 800-53 Appx. J: AR-5(c)
	2.2 Information Classification and Inventory	NIST 800-53 Appx. J: SE-1 NIST 800-60: 3.0 NIST 800-122: 3.1
	2.3 Sensitive and Restricted Information Safeguards	NIST 800-53 Appx. F: AC-16(5), MP-3,6; PE-5 NIST 800-53 Appx. J: DM-1, 2; UL-1 NIST 800-60: 3.0 NIST 800-122: 4.2 45 CFR § 164.310(b), (c) 45 CFR § 164.530(c)(1)
	2.4 Information System Access	NIST 800-53 Appx. F: AC(1), 2(f), (c) 20; AU-9, CA-3, CM-6, 7; IA-1, 4, 5; MP-1, 2, 6, 7; PS-2, SC-1 45 CFR 164.514(d)
	2.5 HCA Computing Devices	NIST 800-53 Appx. F: AC-18, CM-1, 2, 5, 6, 11; PE-1, 3
	2.6 Personal Computing Devices	NIST 800-53 Appx. F: AC-17, 18, 19, 20
	2.7 Network Security	NIST 800-53 Appx. F: AC- 17, CA-9, CM-11(2), SC-15
	2.8 Incident Reporting and Response	NIST 800-53 Appx. F: AU-2, IR-1, 4, 5, 6, 8 NIST 800-53 Appx. J: SE-2 (a), (b)
	2.9 User Information Privacy and Ownership	US Constitution and Common Law
	2.10 Physical Security	NIST 800-53 Appx. F: PE-3, 8
	2.11 Training and Awareness	NIST 800-53 Appx. F: AT-2, 3 NIST 800-53 Appx. J: AR-5(a), (c) NIST 800-122: 4.1.2
	2.12 Data Disclosure	NIST 800-53 Appx. J: AP-1, DI-1(d), DM-2(b), UL NIST 800-122: 4.2.3, 4.2.4 45 CFR § 160.103 45 CFR § 164.502(a)(1)(iii) 45 CFR § 164.506 45 CFR § 164.512(i) 45 CFR § 164.528(a)
3.0	**Administrative Roles**	NIST 800-53 Appx. J: AR
4.0	**Administrative, Technical and Physical Controls**	

	4.1 Confidentiality Agreement	NIST 800-53 Appx. F: PL-4, PS-6 NIST 800-53 Appx. J: AR-5(c)
	4.2 Information Classification and Inventory	NIST 800-53 Appx. J: SE-1, RA-2 NIST 800-60: 3.0 NIST 800-122: 3.1
	4.3 Sensitive and Restricted Information Safeguards	NIST 800-53 Appx. F: AC-16(5), 20; CA-3, MP-1, 2, 3, 6, 7; PE-5 NIST 800-53 Appx. J: DI-1, DM-1, 2; UL-1 NIST 800-60: 3.0 NIST 800-122: 4.2 45 CFR § 164.310(b), (c) 45 CFR § 164.312(c)(2) 45 CFR § 164.530(c)(1)
	4.4 Information System Access	NIST 800-53 Appx. F: AC-1, 2, 11, 12, 20; AU-9, CA-3, CM-6, 7; IA-1, 4, 5; MP-1, 2, 6, 7; PS-2, 3, 4, 5; SC-1 45 CFR § 164.308(a)(3)(ii)(B) & (C), (a)940(ii)(B), (a)(4)(ii)(B), (a)(4)(ii)(C) CFR 164.514(d)
	4.5 HCA Computing Devices	NIST 800-53 Appx. F: CM-6, 10, 11; SI-2, 3
	4.6 Personal Computing Devices	NIST 800-53 Appx. F: AC-5, 17 45 CFR § 164.308(a)(5)(ii)(B)
	4.7 Network Security	NIST 800-53 Appx. F: AC- 17, CA-9, CM-11(2), IA-8, PL-2, SI-3, 4, 5; SC-15
	4.8 Incident Reporting and Response	NIST 800-53 Appx. F: AU-2, IR-1, 4, 5, 6, 8 NIST 800-53 Appx. J: SE-2 (a), (b) 45 CFR § 164.308(a)(6)(ii)
	4.9 User Information Privacy and Ownership	US Constitution and Common Law
	4.10 Physical Security	NIST 800-53 Appx. F: PE-3, 8 45 CFR § 164.310(a)(2)(iv)
	4.11 Training and Awareness	NIST 800-53 Appx. F: AT-2, 3 NIST 800-53 Appx. J: AR-5(a), (b), (c) NIST 800-122: 4.1.2
	4.12 Data Disclosure	NIST 800-53 Appx. J: AP-1, DI-1(d), DM-2(b), UL NIST 800-122: 4.2.3, 4.2.4
	4.13 Asset Inventory	NIST 800-53 Appx. F: CM-8, PE-16 NIST 800-53 Appx. J: SE-1 (a), (b) 45 CFR § 164.310(d)(2)(iii)
	4.14 Change Control	NIST 800-53 Appx. F: CA-6, CM-1, 2, 6, 10 NIST 800-53 Appx. J: DI-2
	4.15 Contingency Planning	NIST 800-53 Appx. F: CP-1 through 13
	4.16 Acquisition, Maintenance, Sale, Movement or Disposal of Hardware	NIST 800-53 Appx. F: CP-2, 9; MA-2, 6; MP-8, SA-4, 5, 9 45 CFR § 164.308(a)(2)(i), (a)(7)(ii)(A) & (C), (d)(2)(i) 45 CFR § 164.310(d)(2)(ii) 45 CFR § 164.312(a)(2)(ii)

	4.17 Security Risk Assessments	NIST 800-53 Appx. F: CA-2, CM-4, RA-1, 3; SA-3 45 CFR § 164.308(a)(1)(ii)(A) & (B), (a)(8) 45 CFR § 164.316(b)(2)(ii) & (iii)
	4.18 Privacy Impact Assessments	NIST 800-53 Appx. J: AR-2 (a), (b); AR-3 (b) 45 CFR § 164.316(b)(2)(3), (b)(2)(ii) & (iii)
	4.19 Audit and Accountability	NIST 800-53 Appx. F: CA-7, AU-1, 3, 5, 6, 8, 11 45 CFR § 164.308(a)(1)(ii)(D) 45 CFR § 164.312(b)

APPENDIX B

INFORMATION SECURITY AND PRIVACY POLICY ACKNOWLEDGMENT AFFIDAVIT

I Hallie Morgan hereby affirm and acknowledge that I have read and understand the West Virginia Health Care Authority's Information Security and Privacy Policy.

I hereby affirm and acknowledge that I accept and will abide by this policy. Additionally, I understand that any violation of this policy may result in some form of disciplinary action, up to and including dismissal. No statement or representation, either oral or written, can supplement or modify this guide without the express written consent of the Executive Director or Board Chairperson.

Should circumstances arise where the interpretation of this policy is required, the Legal Department shall be solely authorized to provide such interpretation.

Acknowledged and Accepted

Hallie Morgan 2/23/24

Signature *Date*

WVHCA Adjudication Requirements

This document describes the processing requirements adjudication of the WVHCA master dataset:

Purpose:

On a periodic basis, provide the WVHCA with an adjudicated dataset based on the master claims dataset, essentially accumulating data across claims as applicable, adding new information such as DRG grouping and identifying which claim records are "analytic" and/or "combined".

- The adjudicated dataset will be a year-to-date claims dataset containing all claims submitted (except rejected claims) and any new, combined claims we create as a product of adjudication.
- Adjudication essentially means that we will create new, combined claim records by accumulating data across interim and/or late charge claims for a given episode of care.
- Adjudication also means that we will determine which of multiple claims for any given discharge gets flagged as the "analytic record" containing the complete billing information.
- We will also add information to the claims which add value to the analytic process, including but not limited to DRGs, MDCs, County Type, Age Groups, etc.

Requirements:

- The adjudicated dataset will be a calendar year-to-date dataset based on the master dataset at the time the adjudicated dataset is generated.
- The adjudicated dataset will be generated on a weekly basis. However, the adjudication process will be reviewed on a quarterly basis, preferably post reconciliation of the master dataset to improve the quality of the adjudicated dataset.
- The adjudicated dataset will contain all master dataset claims and any new, combined claims generated by the adjudication process.
- Create combined claims where charge adjustments or complete sets of interim claims exist (see "Claims Processing", below)
- Most data elements for the adjudicated data set are data elements simply carried forward from the master dataset and need no further explanation here. Some of the new data elements which are added to the adjudicated dataset are completely defined in the document e.g., BILLCAT or DISCTYPE and again, need no further explanation here. Those data elements requiring more detailed explanation are discussed here:
    - MASTERF "Flag records for master file"
        - Flag all claims carried forward from the master dataset
    - ANFLAG "Flag records for analysis file"
        - Where multiple claims exist for a given discharge, flag one claim as the analytic record (unless deleted by xx8)

        - New claims created by combining interim (xx4, xx3, xx2) or late charge (xx5) claims are flagged as the analytic record
        - xx0 and/or xx6 claims are never flagged as analytic records
    - COMBFLAG "Flag new combined records"
        - Flag new claims generated by combining or accumulating claims during adjudication
    - COMPLETE "Y - complete discharge"
        - Flag all interim claims (xx4, xx3, xx2) used to generate a new combined claim
    - B_MONTH "Billing month flag for the current year"
        - A 12 character code of the form "123456789ABC" representing the calendar months January through December based on the SDATE and EDATE coded each claim
        - For new claims combined from xx4, xx3, xx2 claims, B_MONTH is based on the accumulated SDATEs and EDATEs and may result in non-contiguous periods i.e., "1 3" when January and March are present but February is missing in the data)
- Only the first 45 ancillary revenue buckets (code|charges|units) are in the adjudicated dataset's "master" file. When the count of ancillary revenue buckets exceeds 45, output the excess ancillary revenue buckets (46+) to the "master2" file of the adjudicated dataset.

Claims Processing:

A) stand-alone bill type (xx1)
B) interim bill processing for first, continuing, and last claims (xx2, xx3, xx4)
C) transaction processing for late charges, replacements and voids (xx5, xx7, xx8 which adjust, replace or void claims)
D) Medicare Part A and B (combination of x1x and x2x)

Bill Type Definitions:

xx0 – complete claim, no charge (e.g., charity care)
xx1 – complete claim with charges; covers admit date through discharge date
xx2 – interim, first claim; begins with admit date
xx3 – interim, continuing claim
xx4 – interim, last claim; ends with discharge date
xx5 – late charge claim; additional charges to a prior complete claim
xx6 – reserved
xx7 – replacement of prior claim; completely replaces a prior complete claim
xx8 – void of prior claim; eliminates a prior complete claim (which may or may not be replaced)

A. Stand-alone Bill Type

The xx1 bill type is complete and is accepted as is. The xx1 bill type may be further modified by transaction processing, generating a new combined claim (if not deleted by an xx8 bill type). About 99% of the claims meet this category. The rest of the claims go through the process described below.

B. Interim Bills: Building a Final Bill

Only hospitals with unique PROV/PATNOs are allowed to process interim bills. PROV/PATNO is the identifier which ties the components together to build a complete bill.

Required Components. At a minimum, a built bill is composed of data from BTYPEs xx2 and xx4. It may include xx2, xx3 (one or many), and xx4. Whenever an xx4 is determined to be matched to a corresponding xx4 (plus any xx3 continuing claims), the process creates a new combined xx1 claim and adds it to the adjudicated dataset. All interim bills share the same PROV, PATNO, BILLCAT, and ADMIT. It should be noted that interim bills may not share the same EDATE or SDATE but must always share the same ADMIT.

How Components Are Combined. Depending on the nature of a field, combining the data from xx2, xx3, and xx4 claims into a new combined claim takes one of these forms:

1) Use Last Instance

For most fields which should contain a single instance, e.g., PROV, it is taken from the xx4 claim without examining whether the value occurs or differs in any other claim in the series.

> One exception: for attending and operating physician (NPI_ATT & NPI_OP), we'll use the values we find on the xx4 bill. However, we'll also check the xx2 and all xx3's and if there are any other unique physician Ids in any of these, we'll add up to two "other physicians" (NPI_OTH1 & NPI_OTH2) should they be empty on the xx4

2) Use First Instance
For selected fields which are only expected to occur on the first claim, e.g., SDATE, it is taken from the xx2 bill type (without examining whether the value occurs or is different in any other xx3 or xx4 bill type).

3) Use All Unique Instances
For certain fields which may contain many instances, e.g., secondary diagnosis, we will pull all unique values from all interim claims (xx2, xx3 and xx4).

4) Use All Instances
For certain fields which may contain many instances and where duplicate values are allowed, e.g., other procedures, we will pull all values from all interim claims (xx2, xx3, and xx4).

5) Sum Values From All Instances
For certain fields which data can be reasonably aggregated (typically summed), e.g., revenue code charges, we will sum all values for each unique related field (in this example, sum all charges for any one revenue code) from all interim claims.

The rule applied to each field is contained in the XLS attachment. This document shows which bill types contribute to each field's value in the built claim.

C. Transaction Processing
Bill type xx5 (late charges) will be processed if the matching xx1 (or xx7 in specific instances) claim exists. Adding charges or changing them is straightforward using the "Sum Values From All Instances" methodology described above. However, if the claim to which they apply is not found, the xx5 bills are not processed.

xx7 bill types (replacements) are processed as the in place of an xx1 claim, whether or not the record it replaces could be found in the dataset, unless it is voided by an xx8. It should be noted that xx7s supersede xx1s which occasionally supersede xx4. Replacements make up about 70% of all the bills that need to be adjusted.

xx8 bill types (voids) are historically rare. xx8 bill types will cause the matching claim to be voided.

Adjudication Rules:

It is the intention of this process to collect and adjudicate claims data containing the most current information which represents all discharges from all facilities using the following rules:

All master dataset records are adjudicated first (setting of the master, analytic, complete and combined flags as appropriate) and then, once having been added to the adjudicated dataset, amended with additional data elements such as DRGs, age categories, payor types, county information, etc.

As evidenced by the 2006 and 2007 claims data in hand, the vast majority of claims (>90%) group to a single record, mostly xx1 claims:

- These single claim records are added to the adjudicated dataset "en masse".
- There, the single xx1 and xx7 claim records are flagged as analytic records (ANFLAG=1) and all are flagged as coming from the master dataset (MASTERF=1).
- None are flagged as complete or combined (COMPLETE, COMBFLAG).
- Non-xx1 and xx7 claims are individually recorded to the Incomplete Claims table for later analysis with the comment "Orphan claim".

This leaves sets of 2+ claim records per patient to be adjudicated (<10% of the total).

Grouping of claims for adjudication:

For efficiency purpose, all claims are separated into the four claims processing groups:stand-alone bills, interim bills, transaction processing for late charges, replacements and voids, and Medicare Part A and B bills. Then a bill sequence is created to enable the application of adjudication rules. Bill sequences are created by grouping sets of records by PROV, PATNO, BILLCAT, and EDATE. The only exception is for interim bills where ADMIT is used instead of EDATE.
The following table shows an example of the bill sequence construction for transaction processing for late charges, replacements and voids.

Record #	PRO V	PATNO	EDATE	BTYPE	Bill Sequence
1	543210	123456789	01/10/2012	111	111 117
2	543210	123456789	01/10/2012	117	111 117
3	543210	123456789	05/28/2012	111	111 115
4	543210	123456789	05/28/2012	115	111 115
5	543210	987654321	3/24/2012	111	111 117 118
6	543210	987654321	3/24/2012	117	111 117 118
7	543210	987654321	3/24/2012	118	111 117 118

The following table shows an example of the bill sequence construction for interim bills.

Record #	PROV	PATNO	ADMIT	BTYPE	Bill Sequence
1	543210	123456789	01/10/2012	112	112 113
2	543210	123456789	01/10/2012	113	112 113
3	543210	123456789	05/28/2012	112	112 114
4	543210	123456789	05/28/2012	114	112 114
5	543210	987654321	3/24/2012	112	112 113 113 114
6	543210	987654321	3/24/2012	113	112 113 113 114
7	543210	987654321	3/24/2012	113	112 113 113 114
8	543210	987654321	3/24/2012	114	112 113 113 114

The following table shows an example of the bill sequence construction for Medicare Part A and B bills.

Record #	PRO V	PATNO	EDATE	BTYPE	Bill Sequence
1	543210	123456789	01/10/2012	111	111 121
2	543210	123456789	01/10/2012	121	111 121
3	543210	123456789	05/28/2012	211	211 221
4	543210	123456789	05/28/2012	221	211 221
5	543210	987654321	3/24/2012	111	111 117 121
6	543210	987654321	3/24/2012	117	111 117 121
7	543210	987654321	3/24/2012	121	111 117 121

Based on these bill sequences, we apply the adjudications rules outlined in the following section.

Adjudication of grouped claims:

The rules for adjudicating a given set of claims grouped, ordered and segregated by PROV, PATNO, EDATE (ADMIT for interim bills), BTYPE , and bill sequence are:

- Flag all claims in the set as coming from the master dataset (MASTERF=1).
- If an xx8 claim exists:
  - Void all xx4, xx1 and xx7 claims (if any) in that order, keeping the last surviving claim where multiple claims exist.
  - Where only one xx4, xx1 or xx7 claim exists that claim will be voided.
- If an un-voided xx7 claim exists:
  - Void all xx4 and xx1 claims (if any).
- If an un-voided xx1 claim exists:
  - Void the xx4 claim (if any).
- If an un-voided xx4 claim exists and no xx2 exists:
  - Void the xx4 claim.

At this point, only one un-voided xx7, xx1 or xx4 claim may still exist (if any; theoretically, the set could be comprised entirely of any combination of xx2, xx3, xx5 and/or xx8 claims).

- If an un-voided xx4 claim exists:
  - Create a new combined xx1 claim by accumulating the xx2 and xx3 records (if any).
  - Void the xx4 claim (a new combined xx1 claim now exists).
  - Flag the xx4, xx3 and xx2 records as the source for generating the combined claim (COMPLETE=1).
  - Flag the new combined claim as the analytic record (ANFLAG =1).
  - Flag the new combined record as combined (COMBFLAG=1).
  - Move all claims in the set to the adjudicated dataset.
  - *End adjudication of this set of claims.*
- If an xx5 claim exists:
  - If an un-voided xx1 claim exists:
    - Create a new combined xx1 claim by accumulating the xx5 revenue.
    - Void the xx1 record (a new combined xx1 claim now exists).
    - Flag both the xx5 and xx1 records as the source for generating the combined claim (COMPLETE=1).
    - Flag the new combined claim as the analytic record (ANFLAG =1).
    - Flag the new combined record as combined (COMBFLAG=1).
    - Add all claims in the set to the adjudicated dataset.
    - *End adjudication of this set of claims.*
  - If an un-voided xx7 claim exists:
    - Create a new combined xx7 claim by accumulating the xx5 revenue for *unique codes not found on the xx7* and, where a voided xx1 claim exists, accumulating the xx5 revenue *where the difference between the xx1 and xx7 revenue is not greater than or*

equal to the xx5 revenue (i.e., where the xx5 revenue has not already been summed into the xx7 replacement record).

- If no xx5 revenue is actually summed:
  - DELETE THE NEW COMBINED CLAIM.
  - Adjudication will continue with "*If an un-voided xx7 claim exists*", below.
- Else, xx5 revenue was summed with the xx7:
  - Void the xx7 record (a new combined xx7 claim now exists).
  - Flag both the xx5 and xx7 records as the source for generating the combined claim (COMPLETE=1).
  - Flag the new combined claim as the analytic record (ANFLAG =1).
  - Flag the new combined record as combined (COMBFLAG=1).
  - Add all claims in the set to the adjudicated dataset.
  - *End adjudication of this set of claims.*

- If an un-voided xx7 claim exists:
  - Flag the xx7 claim as the analytic record (ANFLAG =1).
  - Add all claims in the set to the adjudicated dataset.
  - *End adjudication of this set of claims.*
- If an un-voided xx1 claim exists:
  - Flag the xx1 claim as the analytic record (ANFLAG =1).
  - Add all claims in the set to the adjudicated dataset.
  - *End adjudication of this set of claims.*

At this point, the analytic claim has not been identified or created so we have, by definition, an incomplete claim. The set of claims must be comprised entirely of any combination of xx0, incomplete(xx2, xx3, xx4), xx5, xx6 and/or xx8 claims).

- Add all claims in the set to the adjudicated dataset.
- Individually record each claim to in the Incomplete Claims table for later analysis with the comment by bill type
  - xx0 "Invalid (charity) claim"
  - xx2 "Incomplete interim, first claim"
  - xx3 "Incomplete interim, continuing claim"
  - xx4 "Incomplete interim, last claim"
  - xx5 "Incomplete late claim"
  - xx6 "Invalid (reserved) claim"
  - xx8 "Incomplete void claim"
- *End adjudication of this set of claims.*

Special Handling for Medicare Part A and B Bills:

Once a combination of Medicare Part A and B (x1x and x2x) is identified, we create a new combined x1x claim by combining the x1x and x2x records. If a replacement, or a late charge, or a void occurs in one of the two bills, the transactional adjustment rules are

applied first prior to combining the two records. If a Medicare Part B (x2x) records does not occur on the same claims as a Medicare Part A records(x2x), we flag the x2x claim as the analytic record (ANFLAG =1). If the total charges are exactly the same on the x1x and the x2x, an xx1 will not be created until it is determined whether the bill is indeed split between two bills or a mistake has been made. These cases will be brought to the attention of the HCA for further investigation.

Appendix A: **Adjudication Issues and Resolutions**

Adjudication Bill Type Combination	**Description of Issue, Impact, Considerations, and Resolution**
xx1,xx7, and xx8 Combination	When this combination of bill types occurs, it is not clear whether the transaction sequence is to replace xx1 by xx7 and then void it by xx8 or to void xx1 and then replace it by xx7. SSS will not apply an analytic flag to the xx1, the xx7, or the xx8 bill type and will bring these cases to the attention of HCA in a report.
Medicare Part A and B (x1x, x2x) combination from Different Hospitals/Units	If Medicare Part A and B claims are from two separates hospitals/units, we apply the analytic flag to both x1x and x2x. When these instances occur, SSS will bring them to the attention of the HCA to determine if a patient transferred or if an incorrect PROV was submitted.
Different Admit Date for the same Discharge	Interim claims are identified based on ADMIT date for the same PATNO. If the ADMIT date is not the same among bill types of the same discharge, SSS will provide this information back the HCA to follow-up with hospitals.
Duplicate Bills	In general, if two of the same bill exist (other than a 113) these will be brought to the attention of the HCA by SSS for review. The most common cases are duplicate interim bills (xx2 and xx4).
Combination of Interim and Final Claims (xx1 with [xx2, xx3, and xx4])	When there is a combination of interim claims (xx2, xx3, xx4) and final claims (xx1), we adjudicate the two separately and may end up with two adjudicated XX1. It is not clear why there would be a mixture of interim and final claims. All cases will be reported to HCA for review.

Appendix B: Summary of Bill Sequences in the November 16, 2012 File

1. Final Bills	
Bill Sequence	**Adjudication Comments**
xx1	Final bill-no adjustment needed. About 99% of the discharges
2. Bills with Late Charges, Replacements, and Void	
Bill Sequence	**Adjudication Comments**
xx1,xx5	
xx1,xx5,xx7	
xx1,xx7	
xx1,xx7,xx8	
xx1,xx8	
xx5	
xx5,xx7	
xx7,xx8	
xx8	
3. Interim Bills	
Bill Sequence	**Adjudication Comments**
xx1,xx2, xx3, xx4	
xx1,xx2	
xx1, xx2,xx4	
xx1,xx3	
xx1,xx3,xx4	
xx1,xx4	
xx2	
xx2,xx3	
xx2,xx3,xx4	
xx2,xx3,xx4,xx7	
xx2,xx4	
xx2,xx7	
xx3	
xx3,xx4	
xx3,xx4,xx7	
xx3,xx4,xx8	
xx4	
xx4, xx7	
Medicare Part A and B	
Bill Sequence	**Adjudication Comments**
x11,x17,x21	
x11,x21	
x11,x24	
x17,x21	
X21	
X24	

Attachment F

Policies Superseded by the Revised *Information Security and Privacy Policy*

These policies are included in the new & temporary employee's packages:

- Information Security Policy (2003)
- Internet/Email/Network Policy (1998)
- Personal Computing Devices (Bring Your Own Device) (2014)

Also superseded:

- **Response to Unauthorized Disclosures Procedure (2013)**
- Patient Identifier Policy Statement 1/14/2008
- Collection of Additional Identifiers in the Hospital Inpatient Uniform Bill (1/1/2014)

These policies are all from 2002 (Superseded by current InfoSec):

- New Employees (training) 4/17/2002
- Data Managers (roles & responsibilities) 4/9/2002
- Department Directors or Delegated Access Coordinators (roles & responsibilities) 4/17/2002
- Information Security Officer (roles & responsibilities) 5/6/2002
- Privacy Officer Job Description (roles & responsibilities) 5/6/2002
- Physical Security Policy 4/9/2002
- Remote Access Policy 4/17/2002
- Preventative Measures, Backup, and Disaster Recovery of Data Assets 4/19/2002
- Data Classification Policy 4/26/2002
- Authorized Data Users 5/6/2002
- Password and Workstation Policy 6/25/2002
- Confidentiality Policy 6/27/2002

WEST VIRGINIA Department of Health & Human Resources

WEST VIRGINIA HEALTHCARE AUTHORITY

Attachment G

West Virginia

Hospital Data Submission System

Data Collection User Manual

West Virginia Hospital Association

January 2022

OVERVIEW

West Virginia Hospital Association utilizes HIDI's (Hospital Industry Data Institute) hospital discharge data collection tool as the cornerstone for its data program. Hospitals submit data through a secure, web-based tool. HIDI data submission tools provide WV defined error checks to assist in ensuring accurate, high quality data to meet hospital and state reporting needs. A series of reports are provided to assist each hospital with information to monitor and manage data submissions.

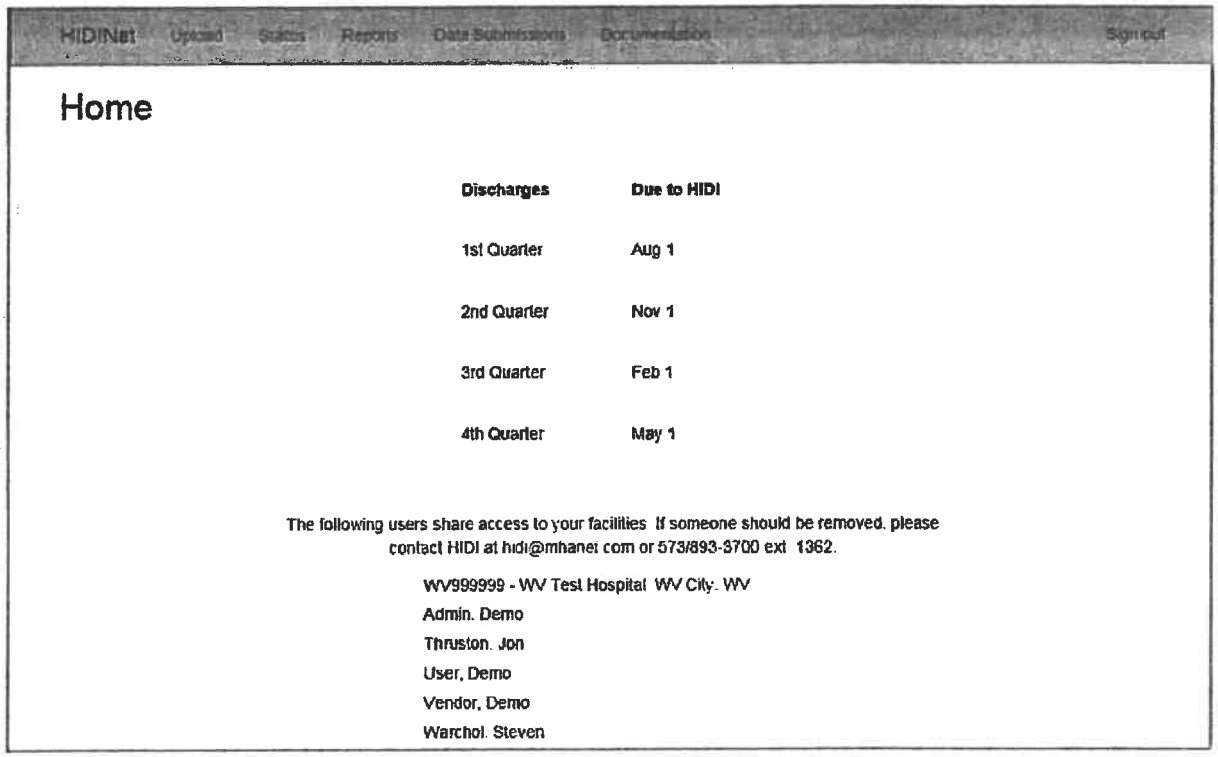
THE PROGRAM

Go to: https://www.hidionline.com/HIDINetV3/

The secure login page will prompt for an email address and password for the system. Due to HIPAA security requirements, each individual user must have their own password for this system.

HOME SCREEN

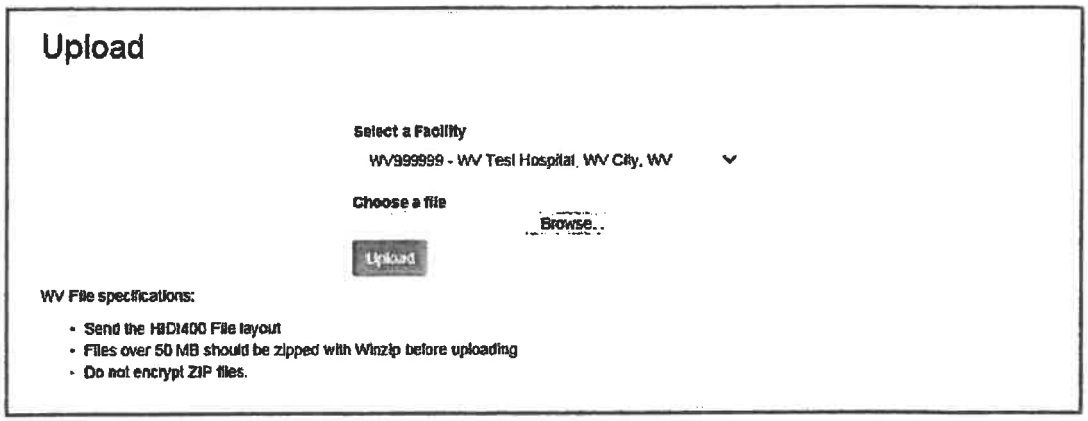
Successful login will open the HOME screen. This screen provides a list of available menu options placed horizontally across the top of the page. This page will display the list of submission deadlines and a list of users authorized to access the account for the facility. Please review the user list and verify the users listed are authorized to access your facilities' data. If changes need to be made, click the "Contact Us" link or email address listed above the user list and send a note stating the required changes and reason for the change. You will be contacted if further information is required.



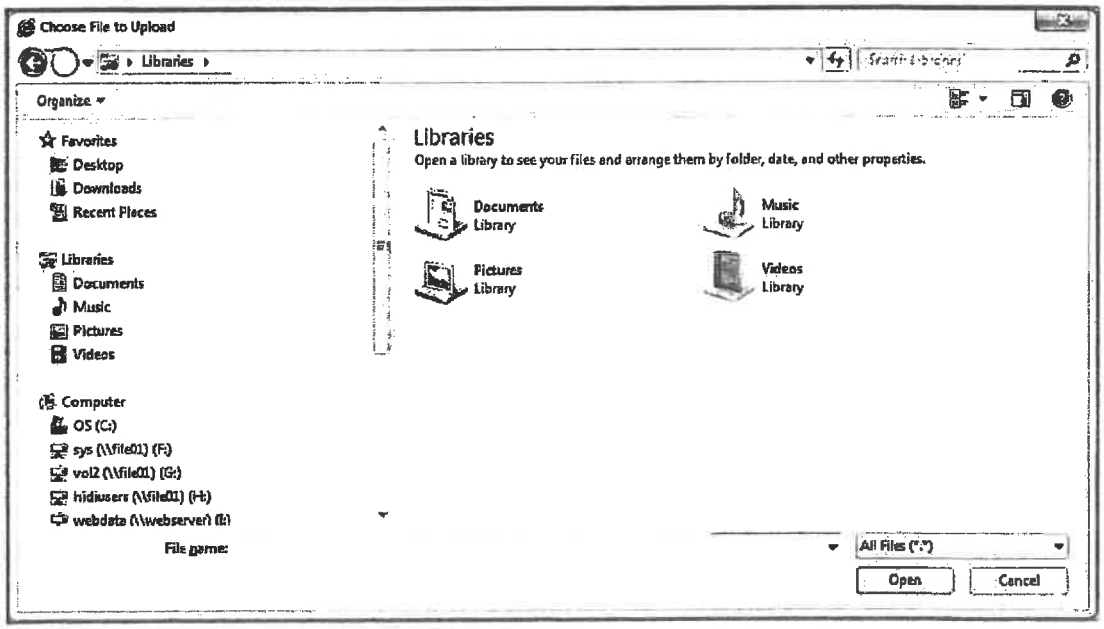
DATA SUBMISSION

To upload a discharge data file to the system, scroll over the "Upload" menu bar and select "UB Discharge Data".

Select the correct facility from the dropdown menu. Some users may see multiple facilities on their drop-down list. Users may be authorized to submit data for multiple facilities but can only submit one data file at a time.



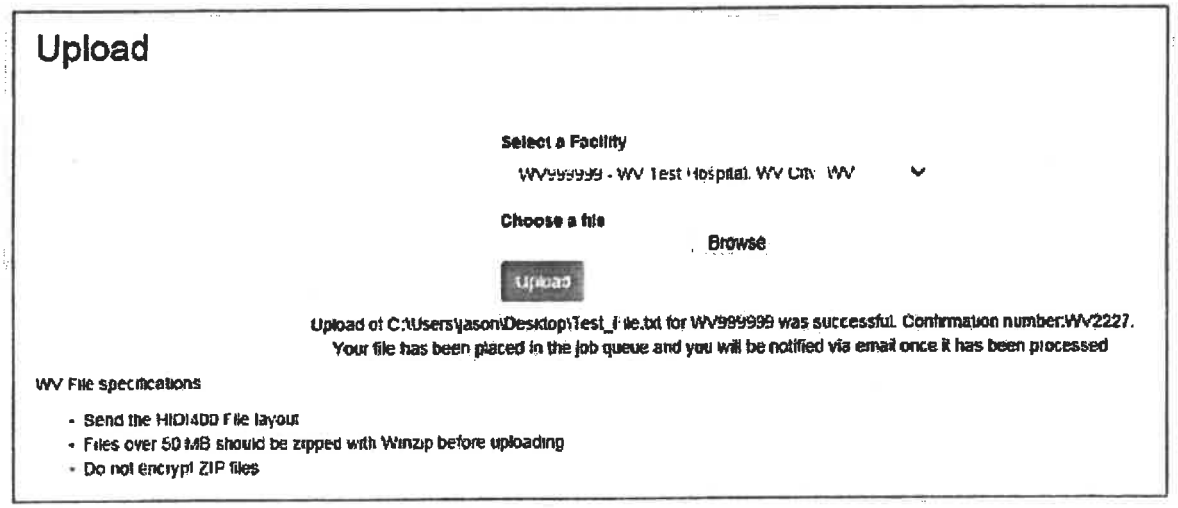
Once the hospital is selected, click the "Browse" button. This opens a browsing screen window where the user can navigate to the proper location and select the discharge data file to be uploaded.



Select the appropriate file and click "OPEN". The file location should display next to the browse button.

Click "Upload" to send this file to the data collection system. Once the upload is complete, the preprocessor will do an initial verification of the file submitted.

If the upload is successful, a message will display the name of the file uploaded and a confirmation number (also called the batch ID). Please record the batch ID when the file is uploaded for later reference.



A message in red states, "If uploading a replacement file, be sure to delete the original from the STATUS page first!" Instructions for deleting a batch are found on page 9.

File types and parameters are listed on the upload page. The file can have any name as HIDI only uses the name for reference. The file size must be less than 50 Megabytes. Zip files can only contain one compressed file and they cannot be password protected. The preprocessor is an automated system, if a password is being used to encrypt a zip file, the processor cannot open and validate your data file.

STATUS PAGE

Click on the "Status" heading.

The Status page shows current and previous 8 quarters of data including record counts, error rates and a link to access the error correction screens for the selected facility.

WV999999 - WV Test Hospital, WV City, WV

	Monthly IP Records			Monthly OP Records			IP Error Rate	OP Error Rate	
Q118	0	0	0	0	0	0	100	0	Correct
Q218	139	156	149	0	0	0	100	0	Correct
Q318	0	0	0	0	0	0	0	0	Correct
Q418	0	0	0	0	0	0	0	0	Correct
Q119	0	0	0	0	0	0	0	0	Correct
Q219	0	0	0	0	0	0	0	0	Correct
Q319	0	0	0	0	0	0	0	0	Correct
Q419	0	0	0	0	0	0	0	0	Correct

The status page also shows IP/OP error rate and the IP/OP record counts separated by quarter.

REPORTS PAGE

Click on the "Reports" heading to see the Edit Detail, Verification and Submit List reports. For each batch processed by the system you will see an Edit Detail report and a Verification report.

A Submit List report is created when the user selects "generate listing" in the Submission Details window. Additional information for this report is found on page 8.

HIDINet Upload Status Reports Data Submissions Documentation

WV999999_EditDetail_Q419.pdf	12/20/2019	11:03:31
[illegible]	11/27/2018	13.35.02
WV999999_Verification_2016.xlsx	03/14/2019	09:24:13
[illegible]	11/04/2019	09.59.00

EDIT DETAIL

To view the list of record errors and other details, click the "Edit Detail" report link.

INPATIENT ERROR SUMMARY REPORT
DISCHARGE PERIOD FROM 4/1/2018 TO 6/30/2018

ERROR#	F/W	ERROR MESSAGE	ERROR COUNT	ERROR RATE	EDIT STATUS
402	F	Primary payer is missing	1	0.22%	ACTIVE
403	F	Payer is invalid	1	0.22%	ACTIVE
1002	F	Patient disposition is missing	8	1.75%	ACTIVE
1301	F	Principal DX POA is missing	1	0.22%	ACTIVE
1304	F	Other DX POA is missing	3	0.66%	ACTIVE
1501	F	Principal DX missing	2	0.44%	ACTIVE
1602	F	Principal PX is invalid	2	0.44%	ACTIVE
1603	F	Other PX is invalid	2	0.44%	ACTIVE
1702	F	Other PX date is missing	1	0.22%	ACTIVE
1707	F	Principal PX date is not between stmt from date and discharge date	1	0.22%	ACTIVE
1708	F	Other PX date is not between stmt from date and discharge date	1	0.22%	ACTIVE
2001	F	Zip code is missing	5	1.09%	ACTIVE
2201	F	Point of origin is missing	1	0.22%	ACTIVE
2203	F	Point of origin is invalid for newborn	3	0.66%	ACTIVE
2508	F	Total charges more than +-5% of line item total	4	0.87%	ACTIVE
2601	F	Attending physician missing	1	0.22%	ACTIVE
3301	F	Patient SSN is missing	1	0.22%	ACTIVE
3701	F	Revenue code is missing	1	0.22%	ACTIVE
3801	F	Revenue units missing	1	0.22%	ACTIVE
4101	F	Bill type is missing	14	3.06%	ACTIVE
4501	F	Admit DX is missing	2	0.44%	ACTIVE
4502	F	Admit DX is invalid	1	0.22%	ACTIVE
5203	F	Statement from date is prior to admit date	4	0.87%	ACTIVE
6002	F	Medicare number is invalid	458	100.00%	ACTIVE
6303	F	Facility NPI is not on file	458	100.00%	ACTIVE
404	W	Payer is missing	2	0.44%	ACTIVE
407	W	Patient Age >= 65 and primary payer not Medicare	23	5.02%	ACTIVE
1202	W	Length of stay greater than 3 years	1	0.22%	ACTIVE
1203	W	Length of stay greater than 90 days	1	0.22%	ACTIVE
1204	W	Length of stay not equal to R&B units	12	2.62%	ACTIVE
1303	W	Principal DX POA reported, DX code exempt	7	1.53%	ACTIVE
1306	W	Other DX POA reported, DX code exempt	101	22.05%	ACTIVE
1520	W	Principal DX indicates poisoning or injury, no ECM code present	5	1.09%	ACTIVE
1521	W	Other DX indicates poisoning or injury, no ECM code present	15	3.28%	ACTIVE
1530	W	ECM code is invalid as other DX	1	0.22%	ACTIVE
1601	W	Operating physician, but no principal PX	197	43.01%	ACTIVE

RPT061 6/27/2018 7:05:10 PM
Version M2 ©2018 Hospital Industry Data Institute Page 1

The first page is the Inpatient Error Summary report and shows the error number and error messages. The F/W column notes whether the error is a fatal error (F) or warning error (W). Fatal errors must be corrected before the batch is accepted. Warning errors need to be reviewed for accuracy.

For example, Error 402 above is a fatal error(F) and states "Primary payer is missing" on the record.

The additional pages of the Edit Detail report show a summary of the discharge record details that contains errors. With this information, you can go back to your internal system, correct the errors and resubmit the batch to the HIDI system. Or the error may be corrected in the using the online patient record correction process (instructions begin on page 10).

INPATIENT ERROR DETAIL REPORT
DISCHARGE PERIOD FROM 4/1/2017 TO 6/30/2017

PATIENT #:		TEST11557	BIRTH DATE: 01-03-1973		DISCHARGE DATE	04-03-2017	ATTENDING PHYSICIAN: 1124313556
MED REC:		TEST11557	BILL TYPE:	111	ADMIT DATE:	03-31-2017	
Error No.	F/W	Field Value	Error Message				
3705	I	999	Verify revenue code				
3803	I	1	Verify revenue units				
3901	F	$0.00	Revenue charge is missing				
PATIENT #:		TEST10026	BIRTH DATE: 05-22-1991		DISCHARGE DATE	04-20-2017	ATTENDING PHYSICIAN: 1952656977
MED REC:		TEST10026	BILL TYPE:	111	ADMIT DATE:	04-16-2017	
Error No.	F/W	Field Value	Error Message				
9726	I	Z880	Verify other ICD10 diagnosis				
9808	F	Y	POA reported, but other ICD10 diagnosis is exempt				
PATIENT #:		TEST14236	BIRTH DATE: 01-07-1929		DISCHARGE DATE	04-25-2017	ATTENDING PHYSICIAN: 1609937457
MED REC:		TEST14236	BILL TYPE:	111	ADMIT DATE:	04-21-2017	
Error No.	F/W	Field Value	Error Message				
0502	F	X	Sex is not valid				

The example above shows patient number TEST14236 with a submitted invalid sex code. The code submitted was an "X". At this point, you would go back to your patient record on your internal system, replace that invalid sex code with a valid code. Once corrected and completed to your satisfaction, the batch can be deleted on the HIDI collection system and resubmitted with the corrected data. You may also correct the error by using the online patient record correction tool.

A full list of edits is available under the Documentation heading on the Homepage. This document is titled "WV Edit Check Definitions".

VERIFICATION

From the Reports page, click the "Verification" report link. The Verification Report is an Excel document that shows different distributions of inpatient and outpatient records by month and patient data elements.

WV999999_EditDetail_Q419.pdf	12/20/2019	11:03:31
WV999999_Submitted_WV1379.txt	11/27/2018	13:35:02
WV999999_Verification_2018.xlsx	03/14/2019	09:24:13
WV999999_Verification_2019.xlsx	11/04/2019	09:59:00

Data elements include discharges/visits by month, priority of admission, point of origin, patient discharge status, age, sex, race, ethnicity, number of diagnosis codes, number of procedure codes, length of stay, primary payer and payer by Medicare provider number.

6/27/2019

Verification Report - Inpatient
WV999999 - WV Test Hospital - WV City, WV

	Jan-18	Feb-18	Mar-18	Apr-18	May-18	Jun-18	Jul-18	Aug-18	Sep-18	Oct-18	Nov-18	Dec-18
Discharges/Visits												
Inpatient	0	0	0	139	156	149	0	0	0	0	0	0
Priority of Admissio												
1-Emergency	0	0	0	80	83	95	0	0	0	0	0	0
2-Urgent	0	0	0	12	16	11	0	0	0	0	0	0
3-Elective	0	0	0	38	48	29	0	0	0	0	0	0
4-Newborn	0	0	0	9	9	14	0	0	0	0	0	0
5-Trauma Center	0	0	0	0	0	0	0	0	0	0	0	0
9-Information Not A	0	0	0	0	0	0	0	0	0	0	0	0
Missing	0	0	0	0	0	0	0	0	0	0	0	0
Invalid	0	0	0	0	0	0	0	0	0	0	0	0
Point of Origin for A												
1-Non-Health Care F	0	0	0	89	95	79	0	0	0	0	0	0
2-Clinic or Physician'	0	0	0	29	38	40	0	0	0	0	0	0
4-Transfer from a Ho	0	0	0	8	12	9	0	0	0	0	0	0
5-Transfer from a SN	0	0	0	0	0	2	0	0	0	0	0	0
6-Transfer from anot	0	0	0	3	1	3	0	0	0	0	0	0
8-Court/Law Enforce	0	0	0	0	1	0	0	0	0	0	0	0
9-Information not A	0	0	0	0	0	0	0	0	0	0	0	0
D-Transfer from one	0	0	0	0	0	2	0	0	0	0	0	0
E-Transfer from ASC	0	0	0	0	0	0	0	0	0	0	0	0
F-Transfer from a Ho	0	0	0	0	0	0	0	0	0	0	0	0
SN-Born Inside Hosp	0	0	0	8	8	13	0	0	0	0	0	0
6N-Born Outside Ho:	0	0	0	0	0	0	0	0	0	0	0	0
Missing	0	0	0	1	0	0	0	0	0	0	0	0
Invalid	0	0	0	1	1	1	0	0	0	0	0	0

DATA SUBMISSIONS

Click on the "Data Submissions" heading.

Select Facility

WV999999 WV Test Hospital, WV City, WV

Submit Id	Date Received	Low Date	High Date	Status	IP Recs	OP Recs	Skipped	Overlayed	Test	
WV1911	3/5/2019	4/1/2018	6/30/2018	LOADED	458	0	0	0	N	Delete
WV1890	3/5/2019	4/1/2018	6/30/2018	LOADED	458	0	0	0	N	Delete
WV1887	3/4/2019	1/2/2018	3/31/2018	LOADED	542	0	0	0	N	Delete
WV1868	2/21/2019	1/1/2018	1/31/2018	DELETED	682	0	0	0	N	
WV1866	2/21/2019	1/1/2018	1/31/2018	LOADED	34	0	648	0	N	Delete

This page displays the list of the current Batch IDs submitted. The most recent batch submission will appear at the top of the list.

For each batch submitted, the display shows date received, date range contained within the data file, number of records loaded and skipped, and the type of file submitted. The status for each file will change from "Pending" to "Loaded" once the system edit process is complete.

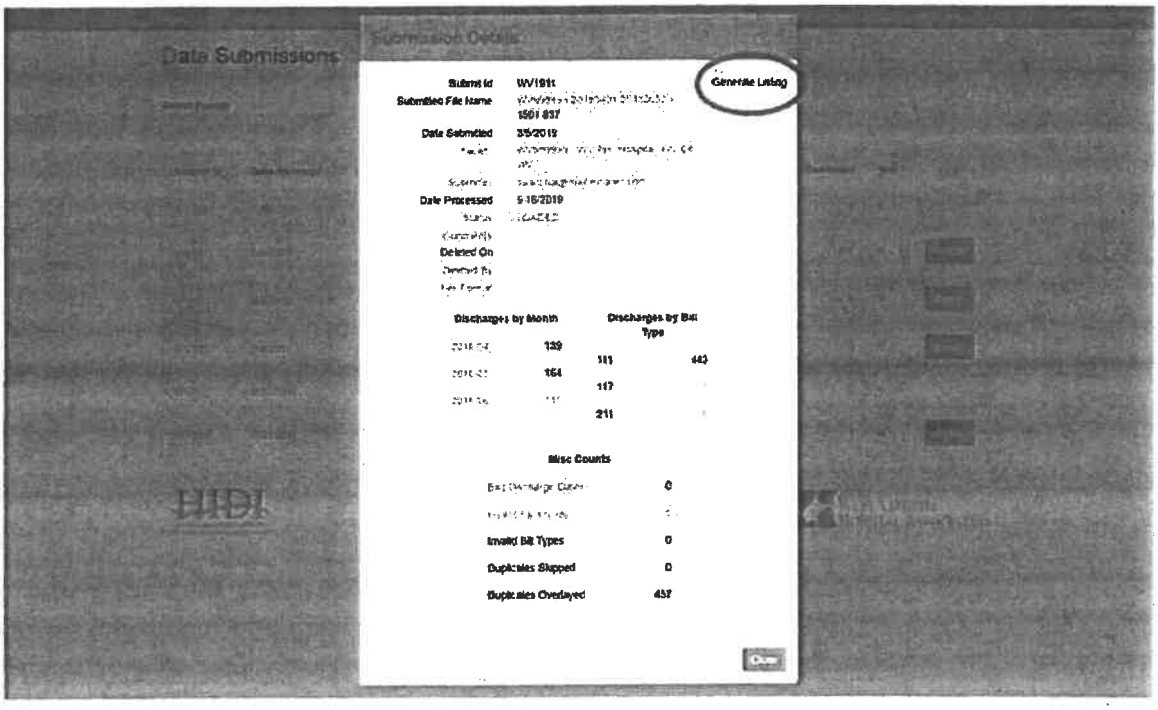
If an error was found by the processor or the analyst and your file was unable to be loaded, the message will show "failed". The system edit process will begin immediately upon file upload. Once the edit process is completed, the user will be notified by email.

To view batch details, click the batch ID link to display the Submission Details report.

The Submission Details report screen displays the batch ID, original filename, submission date, facility Medicare number, user submitting the file, date range of data within the file, date the file was processed, date the file was deleted and the user that deleted it (if applicable), status of the batch and format of the data file received.

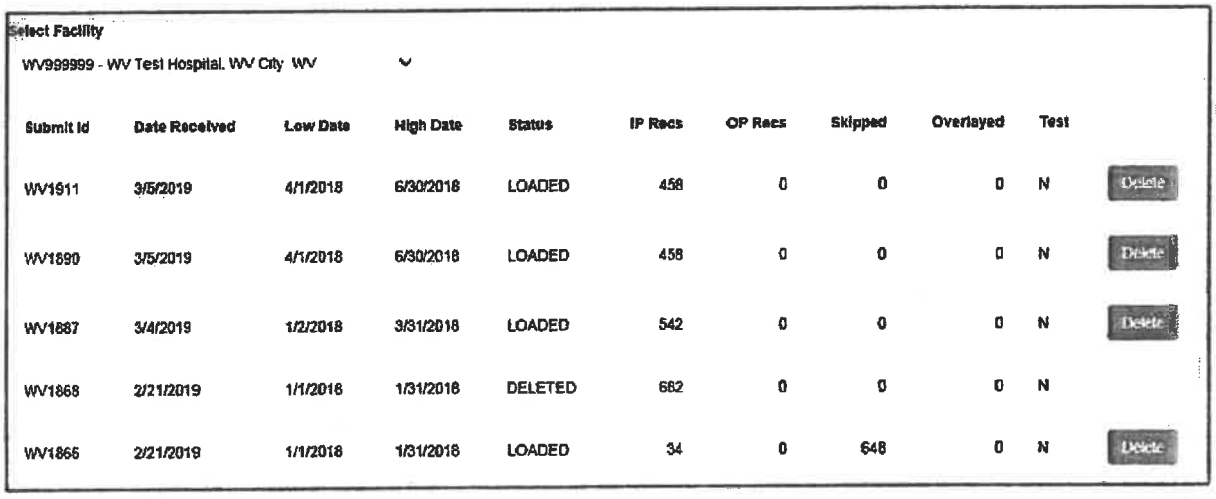
Information on this screen also includes a list of record counts for each bill type, a total record count loaded, a summary of records that were not loaded and a list of record counts by month-year.

Generate Listing Report - The Submission Details report screen also provides a link to generate a report of all accounts included in the batch. User will click on "Generate Listing" (circled below) to create this report. Once the report is created, it will be found under the Reports tab with the report name "Submit List" and related batch number. The Submit List report includes Patient Account Number, Medicare Provider Number, Admission Date, Discharge Date, Bill Type and Payer Code.



TO DELETE A BATCH

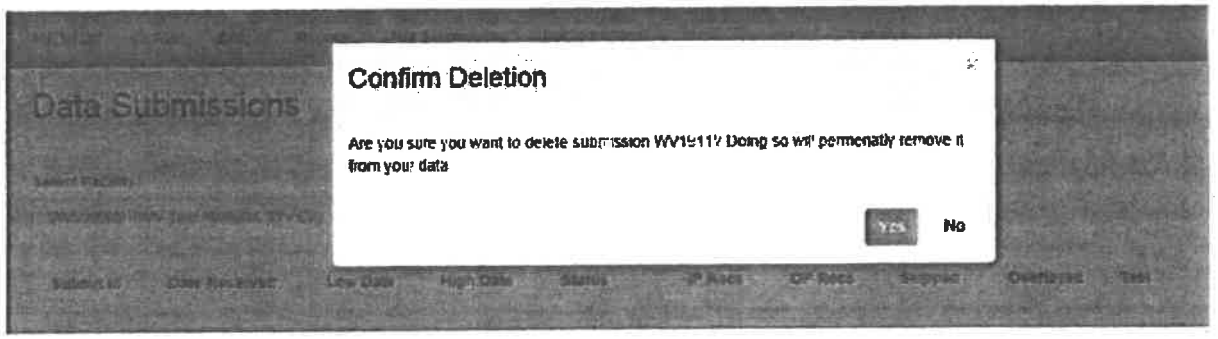
Under the Data Submissions page, as shown below, click "Delete" to the right of the batch status record to delete the batch. A screen will display asking the user "Are you sure?" that must be verified before the batch is deleted.



Select Facility

WV999999 - WV Test Hospital, WV City WV

Submit Id	Date Received	Low Date	High Date	Status	IP Recs	OP Recs	Skipped	Overlayed	Test	
WV1911	3/5/2019	4/1/2018	6/30/2018	LOADED	458	0	0	0	N	Delete
WV1890	3/5/2019	4/1/2018	6/30/2018	LOADED	458	0	0	0	N	Delete
WV1887	3/4/2019	1/2/2018	3/31/2018	LOADED	542	0	0	0	N	Delete
WV1868	2/21/2019	1/1/2018	1/31/2018	DELETED	682	0	0	0	N	
WV1866	2/21/2019	1/1/2018	1/31/2018	LOADED	34	0	648	0	N	Delete



DOCUMENTATION

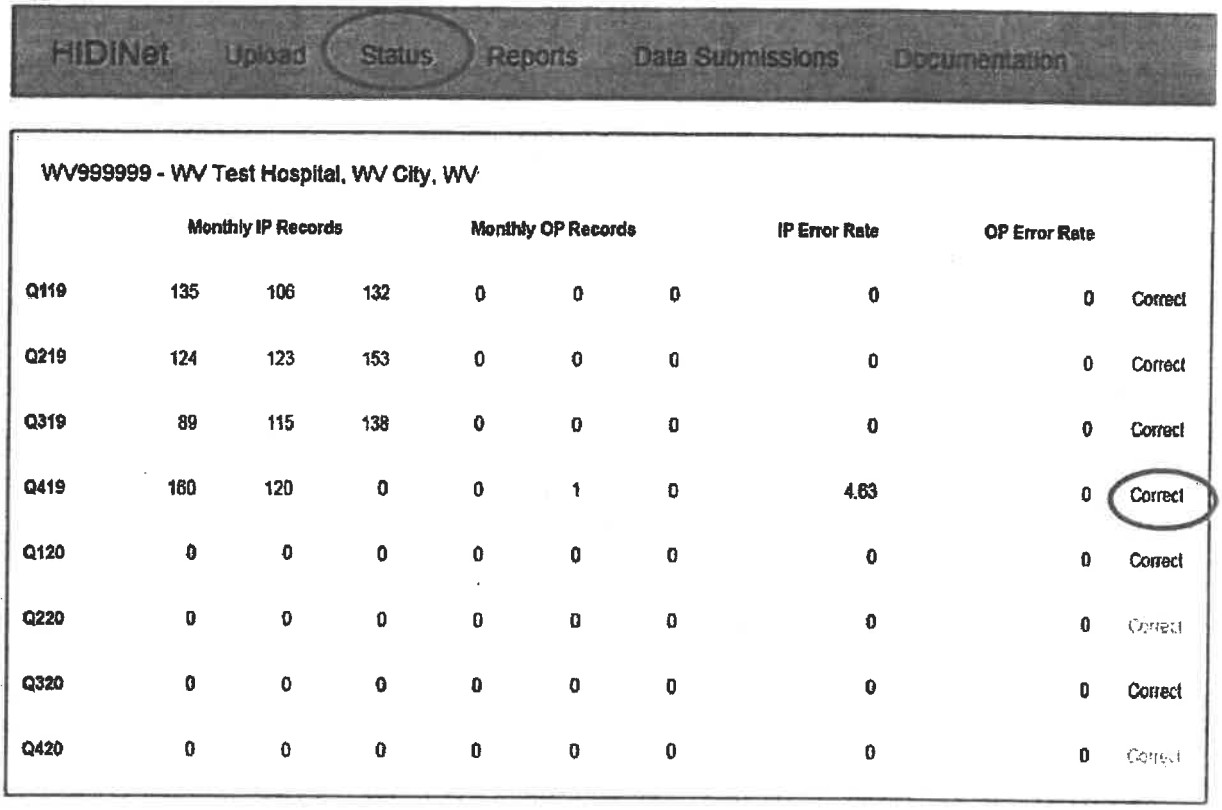
The documentation heading contains additional documentation and instructions. Under this heading, you would find a copy of the instructions along with a training video and other supporting material.

ONLINE PATIENT RECORD CORRECTION

An online correction tool is also available to users. This tool is useful if your hospital does not resubmit data once the initial submission has been sent. We encourage submitters to do corrections within their own system and then delete their batches and resubmit updated. As a reminder, if you make corrections through the online tool, those corrections may be overwritten with erroneous information if data is resubmitted.

STATUS PAGE

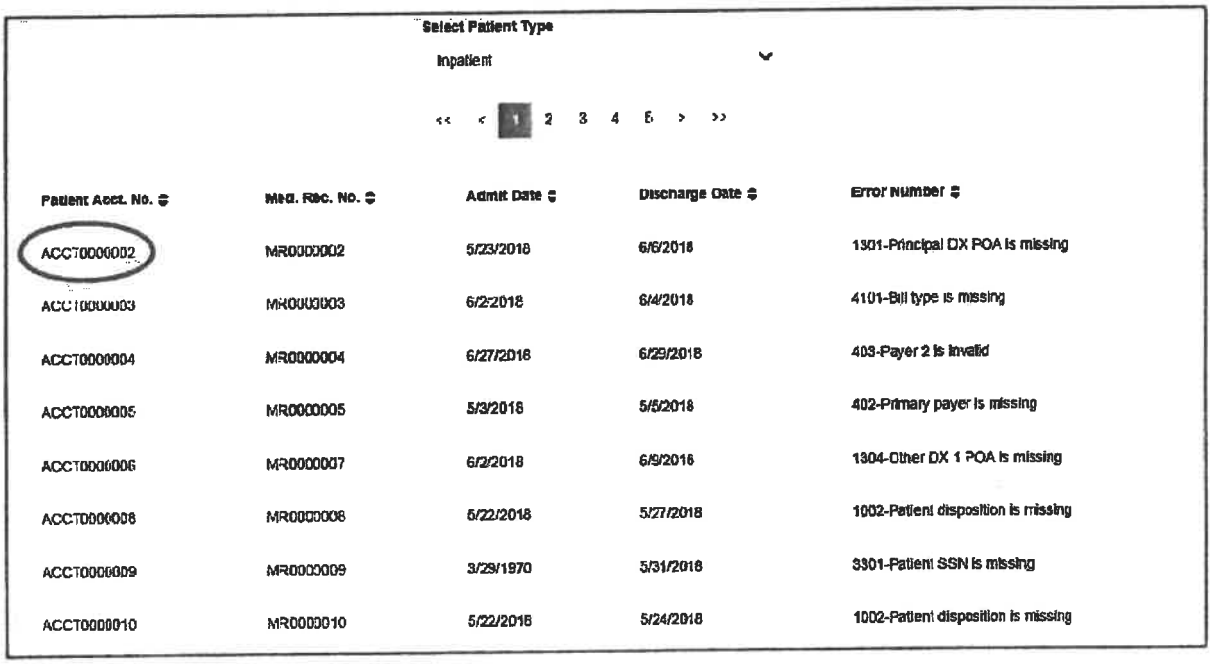
On the Status page, click the "Correct" link.



When the link is clicked, the error list displays. Click the drop-down list to select either Inpatient or Outpatient errors.

ERROR CORRECTION LIST

Click the Patient Acct. No. to access the "Error Corrections" Screen.



Select Patient Type

Inpatient

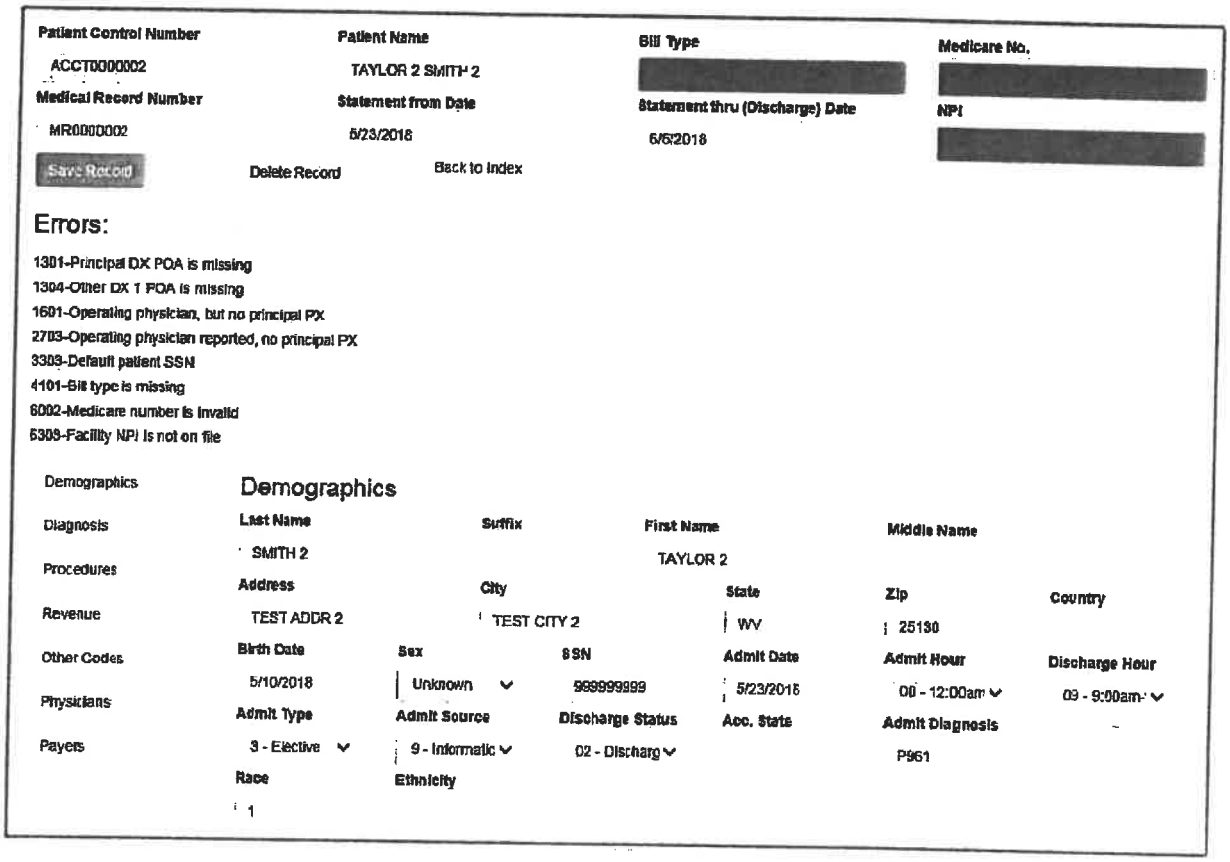
<< < 1 2 3 4 5 > >>

Patient Acct. No.	Med. Rec. No.	Admit Date	Discharge Date	Error Number
ACCT0000002	MR0000002	5/23/2018	6/6/2018	1301-Principal DX POA is missing
ACCT0000003	MR0000003	6/2/2018	6/4/2018	4101-Bill type is missing
ACCT0000004	MR0000004	6/27/2018	6/29/2018	403-Payer 2 is invalid
ACCT0000005	MR0000005	5/3/2018	5/5/2018	402-Primary payer is missing
ACCT0000006	MR0000007	6/2/2018	6/9/2018	1304-Other DX 1 POA is missing
ACCT0000008	MR0000008	5/22/2018	5/27/2018	1002-Patient disposition is missing
ACCT0000009	MR0000009	3/29/1970	5/31/2018	3301-Patient SSN is missing
ACCT0000010	MR0000010	5/22/2018	5/24/2018	1002-Patient disposition is missing

See Next Page for Details.

ERROR CORRECTIONS SCREEN

The corrections screen displays a list of every modifiable field within the patient discharge record. The middle left of the screen displays any Warning or Fatal errors that go with this record. To see expanded record details, click on any of the lower-left sections (Demographics, Diagnosis, Procedures, Revenue, Other Codes, Physicians and Payer). Most of the errors within the record will be highlighted as shown in the example below.



Scrolling down through the record, the field in error will display highlighted in red and yellow. Move the cursor over the error field and the message related to that field will display.

Make the appropriate corrections to the record and click the blue/grey "Save Record" button on the left side. Click "Back to Index" to return to the Error Correction List page. Clicking "Delete Record" will remove the entire patient record from the database.

The update process will run each weekday at noon and weeknight. Login after corrections are keyed and processed to view an updated Edit Detail report. This process can be repeated as often as necessary to correct errors. It is recommended the all errors be corrected in the source system and resubmitted. Remember, if data is resubmitted from the facility billing system and corrections were not made within, the online corrections will be overwritten with the original erroneous data.

Attachment H

The Novetta strategies use the following patient level fields when available:

- Date of Birth
- Name (uses first, middle, and last names)
- Sex / Gender (uses HIDI internal value)
- Social Security Number
- Standardized Address (includes street address, city, state, and zip code after being standardized via USPS information)

There are two different Novetta processing workflows: rebuild and incremental.

1. **Rebuild:** The rebuild process using all the current state level patient master encounter database, the ADT HL7 patient encounter information, and patients from the watchlists that have been processed in the HIDI Advantage platform to rebuild the Novetta MPID.

   Each state level patient master item/row has a surrogate key assigned to it which is the combination of the discharge date and masked values of hospital id, patient account number, account year, encounter type, and state code. The patient master surrogate key is: ddate [formatted yyyymmdd]-MASK_HASH of ([hospital_id]-[patient_account_number]-[account_year]-[in_out]-[state_code]).

   Each ADT HL7 patient encounter summary item is assigned a surrogate key which is [current timestamp (formatted yyyyMMddHHmmss)]_[messageUUID]_[streamId].

   The rebuild process uses the strategies to determine which items are for the same patient. It then uses the earliest surrogate key for each patient and completely rebuilds the patient corpus. Between rebuilds, there is a chance that the Novetta MPID could change based on the information currently in the HIDI Advantage platform. For example, patient A was in the state patient master information last quarter with three (3) encounters (January 5th, January 28th, and February 17th) and these are the only encounters for patient A. Based on the information at that time, the January 5th encounter's surrogate key would be used for the Novetta MPID. During this past month, the hospital deleted/removed the January 5th encounter. The Novetta rebuild process now will assign the January 28th encounter's surrogate key as the Novetta MPID.

2. **Incremental:** The HIDI Advantage platform has two (2) incremental processes: HL7 ADT watchlist roster incremental and the HL7 ADT encounter summary incremental.

   The watchlist roster incremental takes the inbound standard watchlist roster information and compares it to the current patient corpus. If it matches an existing patient, the current Novetta MPID is assigned to the inbound watchlist roster information. If it doesn't match an existing patient, it assigns the earliest inbound standard watchlist roster surrogate key as the Novetta MPID. The watchlist roster surrogate key is 99999999_[watchlist_id]_[member_id]. This process also builds the B table for the A/B matching. Patients are added to the current patient corpus as necessary and new instances are kept and included in the rebuild process

   The HL7 ADT encounter summary incremental takes the inbound HL7 ADT encounter summary information and compares it to the current patient corpus. If it matches an existing patient, the current Novetta MPID is assigned to the inbound HL7 ADT encounter summary information. If it

doesn't match, it assigns the earliest inbound HL7 ADT encounter summary surrogate key as the Novetta MPID and all the inbound instances are added to the current patient corpus and new instances are kept and included in the rebuild process.

Surrogate Key (SK) Information:

File/Schema	Fields Used to Create SK
Combined States (state historical)	[ddate formatted(yyyyMMdd)]-MASK_HASH of ([hospital_id]-[patient_account_number]-[account_year]-[in_out]-[state_code])
HL7 ADT Alerting Messages	[current timestamp formatted (yyyyMMddHHmmss)]_[messageUUID]_[streamId]
Watchlist: ADT Alerting Roster	99999999_[watchlist_id]_[member_id]

Attachment I

WEST VIRGINIA Department of Health & Human Resources

WEST VIRGINIA HEALTHCARE AUTHORITY

West Virginia
Hospital Data Submission System

Data Collection Policies and Procedures

West Virginia Hospital Association

January 2020

West Virginia
Hospital Data Submission System

Data Collection Policies and Procedures

Contents

The West Virginia Health Care Authority (WVHCA) has been charged by the West Virginia Legislature with ensuring compliance with W.Va. Code §16-29B-1 et seq. and the Financial Disclosure Rule, 65 C.S.R. 13. Collection of data for all hospital inpatient stays and outpatient encounters is a part of this duty. Data collected and analyzed through the West Virginia Hospital Data Submission System (HDSS) are used by state and federal agencies, hospitals, universities, and non- profit organizations for health care regulatory and planning purposes. The WVHCA analyzes these data to assess health care access, quality, and cost, as well as disease prevalence and disparities, in West Virginia. This information is used to inform hospital Certificate of Need decisions, and statewide health policy efforts.

This document outlines the required protocols for submission of hospital inpatient and outpatient data to the WVHCA. Additional documents outlining guidelines and specifications for data reporting and editing can be accessed from the WVHCA website at https://hca.wv.gov/fdhome/HospInpatientData/Pages/default.aspx.

I. Data Specifications

A. Hospital inpatient and outpatient data are required to be extracted from billing systems and submitted by all hospitals to the WVHCA in the formats outlined in the *837I Companion Guide* and *Data Element Specifications* documents, which specify the required data file layout and field content.

B. Data must be submitted for all hospital inpatient discharges and outpatient encounters, regardless of the expected source of payment. This is to include, but is not limited to, self-pay and charity discharges, and swing bed discharges. Long term and skilled nursing care discharges should NOT be included.

C. For each inpatient stay and outpatient encounters, the record(s) submitted must represent the final and complete claim. It is recommended that one final record be submitted per discharge, after the claim has been closed.

D. For all inpatient stays that result in a birth, a separate record/claim must be submitted for mother and baby(s).

II. Data Submission and Quality

A. Discharge and encounter records are required to be submitted on a monthly basis within 60 days after the end of the submission month.

B. Data are required to be submitted to the DHHR vendor, the West Virginia Hospital Association, utilizing the Hospital Data Submission System (HDSS), as outlined in the *837I Companion Guide* and *Data Element Specification*.

C. Upon upload to the HDSS, edit checks are performed on the data to assess the completeness and quality of records. Results of the edit checks are displayed in the HDSS and must be reviewed prior to inclusion of the data in the master database. All fatal errors must be corrected while warning errors are provided for consideration and review. A complete list of the edit checks are outlined in the *Edit Check Definitions* guide.

D. As stated in Section I.C, subsequent records can be submitted to adjust, supplement, or void claims previously submitted to the master database. Refer to the *HDSS User Guide* for specific information on revising the master database.

E. Data quality reports (EditDetail and Verification) are available on the data submission and editing website to provide information regarding the completeness and accuracy of submitted data. These reports are designed to assist in the data submission process and should be reviewed regularly to identify and assess data errors. Refer to the *HDSS User Guide* for specific information on accessing and using the DQRs.

III. Reconciliation

A complete and accurate dataset is ensured by conducting data reconciliation at the time of data submission.

A. A Submission Details Report is created for every file uploaded. This report provides the batch ID, original filename, submission date, facility Medicare number, user submitting the file, date range of data within the file, date the file was processed, date the file was deleted and the user that deleted it (if applicable), status of the batch and format of the data file received.
   Additional information on this report includes a list of record counts for each bill type, a total record count loaded, a summary of records that were not loaded and a list of record counts by month-year.

B. The Verification Report is an Excel document that shows distributions of inpatient and outpatient records by month and patient data elements.
   Data elements include discharges/visits by month, priority of admission, point of origin, patient discharge status, age, sex, race, ethnicity, number of diagnosis codes, number of procedure codes, length of stay, primary payer and payer by Medicare provider number.
   Users compare this report to internal reports to validate and reconcile the data uploads.

C. The Submit List report provides a listing of all accounts included in the batch. The Submit List report includes Patient Account Number, Medicare Provider Number, Admission Date, Discharge Date, Bill Type and Payer Code.
   Hospitals use this detailed listing to further investigate any questions or issues that were identified when reviewing the Verification Report.

The Submission Details Report and Verification Reports are created and updated each time data is uploaded or manually corrected. Based on the outcome of the reconciliation process, users may choose to delete the batch and resubmit a corrected file or make corrections to the records using the online patient correction process. Additional details may be found in the *HDSS User Guide*.

Summary reports by hospital are available for monitoring volumes and errors. The WV Health Care Authority and/or their discharge data vendor will work with hospitals to resolve any discrepancies identified.

IV.Compliance

A. Compliance with these policies and procedures is required by W. Va. Code §16-29B-1 *et seq.* and the Financial Disclosure Rule, 65 C.S.R. 13. Facilities are deemed out of compliance if submissions are 120 days overdue or if data quality or format is not in conformity with the required specifications.

B. Noncompliant facilities may be announced in the Health Care Authority's weekly newsletter *Health Care Review*.

V. Technical Assistance

All documentation outlining the required guidelines and specifications for data reporting and editing can be accessed from the WVHCA website at:
https://hca.wv.gov/fdhome/HospInpatientData/Pages/default.aspx

For technical assistance related to the data submission website (HDSS), contact the West Virginia Hospital Association.

Liz Tate
Director, Data Collection and Training
Email: ltate@wvha.org
Office: (304) 353-9710

For additional information related to data reporting policies, procedures, or requirements, contact:
Michael J. Morris
Operation Director
WV Department of Health & Human Resources
Office of Management Information Services
One Davis Square
Charleston, WV 25301
Email: Michael.J.Morris@wv.gov
Office: (304) 356-4129

Exhibit A

West Virginia Hospital Association **CRFQ-0506-MIS2400000001-1**

Vendor's quotation MUST include all costs associated with providing the systems and services described in the RFQ. Costs for travel and webinars must be incorporated into the vendor's fees. No travel or webinar expenses will be reimbursed by the State and are the sole responsibility of the vendor.

Base System Pricing SHALL be a quarterly price and must include all systems and services required to meet the mandatory requirements in Section 3.1 of the RFQ with the exception of Additional Optional System Modules in 3.1.3.2.11 and Optional Services in 3.1.8.

3.1.3.2.11 Additional Optional System Module Pricing SHALL be a quarterly price and must include all systems and services required to expand the scope of the systems to include this optional module. Expansion to include the optional system module is entirely at the discretion of the Agency. If the Agency requests and implements the Optional Systems Module at a time other than the beginning of a billing quarter, the first quarter billing will be prorated to pay for the fraction of the quarter the module is in operation

Optional Services pricing SHALL be an hourly rate that will apply to any of the optional services enumerated in 3.1.8. The decision to utilize optional services is entirely at the discretion of DHHR. 500 hours is a non-binding estimate of the services that might be requested via issuance of an approved delivery order.

BASE SYSTEM	Quarterly Price
HOSPITAL UB DATA SYSTEM (HUBDS)	$65,497.00
ADDITIONAL OPTIONAL SYSTEM MODULE (3.1.3.2.11)	
OPTIONAL SYSTEM MODULE	$20,500.00
OPTIONAL SERVICES (3.1.8)	Hourly Rate
Hourly Rate for all optional services	$2.00

Optional Renewal Year 1	
HOSPITAL UB DATA SYSTEM (HUBDS)	$67,453.00
ADDITIONAL OPTIONAL SYSTEM MODULES (3.1.3.2.11)	
OPTIONAL SYSTEM MODULE	$21,320.00
OPTIONAL SERVICES (3.1.8)	Hourly Rate
Hourly Rates for all optional services	$2.00

Optional Renewal Year 2	
HOSPITAL UB DATA SYSTEM (HUBDS)	$69,480.00
ADDITIONAL OPTIONAL SYSTEM MODULES (3.1.3.2.11)	
OPTIONAL SYSTEM MODULE	$22,173.00
OPTIONAL SERVICES (3.1.8)	Hourly Rate
Hourly Rates for all optional services	$2.00

Optional Renewal Year 3	
HOSPITAL UB DATA SYSTEM (HUBDS)	$71,583.00
ADDITIONAL OPTIONAL SYSTEM MODULES (3.1.3.2.11)	
OPTIONAL SYSTEM MODULE	$23,060.00
OPTIONAL SERVICES (3.1.8)	Hourly Rate
Hourly Rates for all optional services	$2.00