

UBMD Export of Data from Epic Policy

Policy governing the export, storage, transmission, printing, and use of information obtained from the Epic Electronic Health Record.

1. Purpose

The purpose of this policy is to establish requirements and safeguards for the export, storage, transmission, printing, and use of patient and organizational data obtained from the Epic Electronic Health Record (Epic) system. This policy is intended to protect Protected Health Information (PHI), ensure compliance with HIPAA and applicable state and federal regulations, and maintain the confidentiality, integrity, and availability of patient information.

2. Scope

This policy applies to all workforce members, providers, employees, contractors, students, and other authorized users who:

- Export data from Epic reports.
- Store, transmit, or otherwise handle Epic data outside the Epic application.

3. Definitions

PHI (Protected Health Information): Individually identifiable health information protected under HIPAA.

Epic Export: Any extraction of information from Epic, including CSV, Excel, PDF, report output, screenshots, or other electronic formats.

Authorized Fileshare: Organization-approved network storage locations, including S:\PP and S:\UBA and authorized servers at UBMD Neurosurgery and Pediatrics.

4. Policy Statement

Epic data exports shall be permitted only when required for legitimate business, clinical, operational, regulatory, quality, financial, research, denial management, appeals, prior authorization, or reporting purposes and only after appropriate approval and security controls have been satisfied.

Users are responsible for protecting all exported data and ensuring compliance with HIPAA, organizational privacy policies, and applicable data retention requirements.

5. CSV Export of Epic Reports

5.1 Authorization

Users requiring the ability to export Epic report data to CSV format must submit a request through the approved organizational process:

[Data Export from Epic Reports Request Form and Attestation](#)

Access to Epic export functionality shall be granted only after:

- Completion of the required request form.
- Acknowledgment of user responsibilities.
- Approval by the appropriate business owner and/or manager.
- Completion of any required privacy or security training.

5.2 Approved Use

CSV exports may be used for:

- Operational reporting.
- Revenue cycle functions.
- Quality improvement activities.
- Compliance activities.
- Regulatory reporting.
- Business analytics.
- Other approved business purposes.

5.3 Storage Requirements

All data exported directly from Epic or from the Epic remote environment (OmniSSA VDI):

1. Must be stored only on an approved organizational fileshare: S:\PP or S:\UBA and authorized servers at UBMD Neurosurgery and Pediatrics.
2. Must be accessed only from an organization-issued, imaged and managed laptop or workstation.
3. Must not be stored on local hard drives, desktop folders, downloads folders, personal cloud storage services, or home computers.
4. Must not be stored on removable media, including USB drives, external hard drives, memory cards, or portable storage devices.

5.4 Minimum Necessary Standard

Users shall export only the minimum amount of data necessary to complete the approved business purpose.

6. Printing of Patient Charts and PDF Records

6.1 Authorized Printing

Printing of patient records and PDF documents from Epic at remote locations that are not UBMD offices may be permitted when required for legitimate business and clinical operations, including:

- Payor denial submissions.
- Medicare appeals.
- Medicaid appeals.
- Veterans Administration (VA) documentation requests.
- Prior authorization submissions.
- Clinical documentation supporting testing or procedures.
- No-Fault insurance claims.
- Workers' Compensation claims.

- Other regulatory or legal requirements.

6.2 Remote Access Considerations

When users access Epic through Horizon/Omnissa VDI and must provide paper documentation to external entities that require physical records, printing may be authorized in accordance with organizational security controls.

Examples include:

- New York Medicare appeal packages that require mailed documentation.
- Payor requests requiring paper records.
- Legal or regulatory submissions requiring printed documents.

6.3 Printing Safeguards

Users must:

- Retrieve printed documents immediately.
- Secure documents from unauthorized access.
- Store printed records in approved locked secure locations.
- Dispose of records using approved confidential destruction methods such as shredding when no longer needed.

Printed records containing PHI shall never be left unattended.

7. Email Transmission of PHI

7.1 Approved Email Requirements

All PHI and HIPAA-regulated information, transmitted via email must:

5. Be sent from an official @buffalo.edu email address.
6. Be transmitted using the organization's licensed ZIX encryption solution.

7.2 Prohibited Email Practices

PHI shall not be:

- Sent using personal email accounts.
- Sent via any method other than licensed ZIX encrypted solutions.
- Forwarded to non-approved systems.
- Shared through unencrypted email methods.
- Sent to recipients without a legitimate business need.
- Sent without checking the correct addressee is the only address listed.

8. User Responsibilities

All authorized users must:

- Complete required privacy and security training.
- Protect exported and printed data from unauthorized access.
- Use exported information solely for approved business purposes.
- Report any suspected privacy or security incident immediately.

- Comply with HIPAA, organizational policies, and applicable laws and regulations.

9. Auditing and Monitoring

The organization reserves the right to:

- Monitor Epic export activities.
- Review user access permissions.
- Audit storage locations of exported and/or printed data.
- Validate compliance with this policy.
- Revoke export privileges when misuse or noncompliance is identified.

All export activity may be logged and reviewed by Information Security, Compliance, Privacy, and management personnel.

10. Violations

Failure to comply with this policy may result in:

- Removal of Epic export privileges.
- Corrective action.
- Disciplinary action up to and including termination.
- Civil or criminal penalties where applicable under HIPAA or other laws.

11. Related References

- HIPAA Privacy Rule
- HIPAA Security Rule
- Organizational Information Security Policy
- Acceptable Use Policy
- Records Retention Policy
- Data Classification and Handling Policy
- Epic Data Export Request Form and Attestation

Acknowledgment

Users granted Epic export access acknowledge responsibility for safeguarding all exported data, adhering to the minimum necessary standard, and complying with all applicable privacy, security, and regulatory requirements.

Understood and Agreed

Employee Signature: _____

Employee Name: _____

Date: _____