

# EINSTEIN MEDICAL CENTER-HEMATOLOGY

**SUBJECT:** HEMATOLOGY STAFF MEETING FEBRUARY/ MARCH

**ATTENDEES:** DAVID HINKLE

**DATE:** MARCH 13, 2017

## AGENDA

CATEGORY	TOPIC	ANNOUNCEMENT / UPDATE	DISCUSSION/ FOLLOW UP
TECHNICAL HEME	1. Mission Story  1. DDR Items  2. MCV Delta update and reminder.  3. CellaVision completed 4. Sysmex XN-10 validated procedure in approval process. 5. Coagulation AV expanded 6. Stago QC/other manual documentation	<ul style="list-style-type: none"> <li>• Does anyone have a story they would like to share?</li> <li>• When you write up a DDR - the DDR should be emailed as an attachment to your supervisor/ or the supervisor of the area that was affected. This should be in a word document. Please ensure the correct form is being used: DDR is AD02-025 Form A4.</li> <li>• DDR big picture report to be posted monthly. We will focus on the highest percentage and focus on how to reduce the biggest causes of DDR's as a team.</li> <li>• MCV delta procedure updated. When a patient is coding release results to nurse, document, and request repeat specimen. REMINDER: Any specimens being cancelled for specimen integrity in question must have a DDR this information is shared with the patient safety committee.</li> <li>• CellaVision LIS Validation complete. Go live is March 21</li> <li>• Sysmex XN1 for CAC is validated and approved for use. Procedure to follow week of 3-13</li> <li>• Coag AV expanded 2-22-17 to achieve greater than 85% AV. Increased % in February, will continue to monitor progress.</li> <li>• We are still having issues with documentation on checklists, maintenance sheets and QC/Calibration sheets. Documentation is required as per our SOP and CAP. Not signing off on maintenance, daily checks or QC is unacceptable. Documenting patient results is a requirement! If you perform a Competency Sample, you must leave the</li> </ul>	Note: Corrections should be called immediately upon discovery and not held.

CATEGORY	TOPIC	ANNOUNCEMENT / UPDATE	DISCUSSION/ FOLLOW UP
General Hematology Updates	<ol style="list-style-type: none"> <li>1. Restocking bench</li> <li>2. Reagent receipt</li> <li>3. Use of idle time</li> </ol>	<ul style="list-style-type: none"> <li>• Restock benches for the next shifts. If something is out, please stock the shelves.</li> <li>• If you receive reagents, please use the log sheets in the bin across from the walk in fridge. Expiration dates, lot numbers and quantity is necessary. Also make sure reagents and supplies away. Do not leave anything in the hallways.</li> <li>• Please use idle time to check inventory. Also check if there is any inventory to be put away.</li> <li>• If you see we are running low on supplies, please continue to notify myself or Ashley.</li> <li>• CAP window – PPE, no cheat sheets. FAQ review are attached to be reviewed.</li> </ul> <p><b>GOALS FOR OUR DEPARTMENT INCLUDE THE FOLLOWING:</b></p> <p><b>Goals for Hematology Department</b></p> <ul style="list-style-type: none"> <li>• ED Coag TAT – Target 90%, RESULTED WITHIN 45 MINUTES</li> <li>• Stat Coag (Hospital) TAT – Target 90% RESULTED WITHIN 55 MINUTES</li> <li>• ED CBC Stat TAT – Target 90% RESULTED WITHIN 45 MINUTES</li> <li>• Stat CBC (Hospital) TAT – Target 90% RESULTED WITHIN 55 MINUTES</li> <li>• Stat Hepnomo TAT – Target 90% RESULTED WITHIN 50 MINUTES</li> <li>• Stroke Stat CBC TAT- 92% RESULTED WITHIN 30 MINUTES</li> <li>• Stroke Stat Coag TAT- 92% RESULTED WITHIN 30 MINUTES</li> <li>• Correlation of Body Fluid to Cytology – Target 100% CORRELATION</li> <li>• Critical Results Called – 100% COMPLIANCE WITHIN 60 MINUTES</li> <li>• Corrected Reports – 98 % COMPLIANCE</li> <li>• CAP – 100% COMPLIANCE</li> <li>• Admin Goal: Tracking ER cancellation times. ER specimens should be cancelled within 60 min of receipt.</li> </ul> <p><b>All QA dashboards are now displayed in the hallway outside the core lab</b></p>	
EMPLOYEE ISSUES/ Competency	<ol style="list-style-type: none"> <li>1. EMCP- employees due for competency Evaluations</li> </ol>	<ul style="list-style-type: none"> <li>• Please remember it is your responsibility to provide the supervisor with all necessary documentation for your competency. Ashley, Loretta and Chris will still provide staff with the unknown samples. Anyone who is competent may observe and sign you off on the duties. It does not have to be a lead tech. Their initials are required when observing</li> <li>• Competency quizzes will continue to be assigned via MEDTRAINING.ORG</li> </ul>	<ul style="list-style-type: none"> <li>• Discussed</li> </ul>


CATEGORY	TOPIC	ANNOUNCEMENT / UPDATE	DISCUSSION/ FOLLOW UP
HOSPITAL NEWS	<ol style="list-style-type: none"> <li>1. Overtime Approval</li> </ol>	<ul style="list-style-type: none"> <li>• Remember you need a supervisor's approval to work over your scheduled time. This is even if it is 15 minute. <b>You must request approval prior to staying</b>, do not let us know that you stayed after your scheduled time. Do not document on payroll exception sheet without approval</li> </ul>	<ul style="list-style-type: none"> <li>•</li> </ul>
HEALTHCARE BUSINESS LITERACY TRAINING	Additional classes	<ul style="list-style-type: none"> <li>• Employees must complete a Voluntary Overtime Acknowledgment Form for each voluntarily worked shift that they accept that is outside of the agreed to, predetermined and regularly scheduled work shift. (Appendix A). Managers must retain the completed Voluntary Overtime Acknowledgment Form for three (3) years. Sheets will be located by the schedules in a separate bin. For those of you that are helping pick up shifts please remember to complete the voluntary overtime form.</li> <li>• Committee that is reviewing the patient progression throughout the organization; It was suggested that a patient tracker be done where someone sits with a patient and time everything that is done. The purpose of this is to show bottle necks and identify opportunity for improvement. STAT-TAT is 60 min once the specimen is received in the lab. Make sure you are canceling in a timely manner (hemolysis, QNS)</li> <li>• Patient safety Fair 3-13 from 7am to 11am</li> </ul> <p>We will be having 2 additional sessions for the Healthcare Business Training that we will hold in the Lab Conference Room. On 3/28 and 3/30 we will have a session from 10am-11am. Anyone who can go should. If you are not able to make these sessions, please log on to the E2 and register for a future class.</p>	
HUMAN RESOURCES	Open Positions Vacancies  Closed Vacancies  Attendance Policy and PSL	<p><u>Open Positions-</u></p> <ul style="list-style-type: none"> <li>• Req # 15930 21406FT-Lab technologist replacing Shiji Johnson</li> <li>• Req #15656 21406-PRN Tech replacing Dueana Hicks</li> <li>• Req #15577-21404-PRN replacing Carmalita Dennis</li> <li>• Req #15655-21404-PRN replacing Karen Hendricks</li> <li>• Req #15806-21410-General Lab Supervisor Blood Bank replacing Pettina Walton</li> <li>• Req# (0-21404-PRN Med Tech-replacing Chizoba Stake</li> <li>• Req# (0-21406-FT Med Tech-replacing Atkia Abdullah</li> </ul> <p><u>Lab - Open Requisitions OPEN REOS. – EMCP/EP</u></p> <p><u>Closed Positions</u></p> <ul style="list-style-type: none"> <li>• Req#15685- Medical secretary II replacing J. Baker 21400- Awarded to external Tamika Green start</li> </ul>	

CATEGORY	TOPIC	ANNOUNCEMENT / UPDATE	DISCUSSION/ FOLLOW UP
		<p>date 3/20/17</p> <ul style="list-style-type: none"> <li>• Req #15354 21406-PRN night shift-Awarded to internal C. Stake.</li> <li>• Req #15355 21406-PRN night shift-Awarded to Jonathan Lam.</li> <li>• Req #15393-21420-Lab Clerk replacing Amy Green-PRN-Awarded to external Lyrika Smalls start date 3/20/17</li> </ul> <p>Employees are allowed to utilize 40 hours of PSL time per calendar year. You may have more accrued however once 40 hours is used call outs will be counted as incidents. Clocking in one minute late is late.</p>	
STUDER	<ol style="list-style-type: none"> <li>1. SLR</li> <li>2. Studer</li> </ol>	<ul style="list-style-type: none"> <li>• What tools do you need to do your job?</li> <li>• Please make sure to congratulate Ethel the first Employee of the month. She will be recognized on the board outside of the administrative offices</li> <li>• New postings on the Studer board: <ul style="list-style-type: none"> <li>◦ Follow up from the employee satisfaction survey will be posted and updated. Our focus is employee appreciation and teamwork.</li> </ul> </li> <li>• 2017 pillar goals are posted</li> <li>• Bathrooms are now unisex.</li> </ul>	<ul style="list-style-type: none"> <li>• Working on Phone list numbers</li> <li>• Store room items gauze, transfer pipettes.</li> </ul>
SEVERE WEATHER	<ol style="list-style-type: none"> <li>1. Review HR02.09 staffing emergency plan</li> </ol>	<ul style="list-style-type: none"> <li>• Please review the attachment HR02.09 staffing emergency plan. Lab staff are considered level 1. We are supposed to receive significant snowfall within the next 24 to 48 hours please be prepared to come to work, and stay if needed. Cots are available in the back room next to the pathology office. Please bring a pillow if needed.</li> </ul>	
ADMINISTRATIVE POLICY REVIEW	<ol style="list-style-type: none"> <li>1. Cell Phone policy-A0181</li> <li>2. Lab PTO</li> <li>3. Review attachments in MTS</li> </ol>	<ul style="list-style-type: none"> <li>• Cell phone usage is unacceptable in the lab during work hours</li> <li>• Submission date of February 28th for personal time off from April 1st through September 30th.</li> <li>• Submission date of August 31st for personal time off from October 1st through March 31st.</li> <li>• Attached: AO214.2; AO222.3; AO270.1; AO301; Label Change notification.</li> </ul>	

### Patient Label Changes – Effective February 20, 2017

Effective Monday, February 20, the format of the patient “sticky” labels will change. The current format lists the first and last name together on the first line. This can cause some letters to be truncated if the name is longer than 24 characters. For easier and more accurate patient identification we will be splitting the name so that the Last Name appears on the first line and the First Name appears on the second line. This will move all other information down one line as well. Please see the examples below.

#### **Before:**

 TESTPATIENT, ELIZABETHGIR DOB: 10/25/2016 00:16 F DOS: 10/25/2016 ATT: MASSEY MD, JULIE S FIN: 77777778 MRN: 101275109	 TESTPATIENT, ELIZABETHGIR DOB: 10/25/2016 00:16 F DOS: 10/25/2016 ATT: MASSEY MD, JULIE S FIN: 77777778 MRN: 101275109	 TESTPATIENT, ELIZABETHGIR DOB: 10/25/2016 00:16 F DOS: 10/25/2016 ATT: MASSEY MD, JULIE S FIN: 77777778 MRN: 101275109
  TESTPATIENT, ELIZABETHGIR DOB: 10/25/2016 00:16 F DOS: 10/25/2016 ATT: MASSEY MD, JULIE S FIN: 77777778 MRN: 101275109	 TESTPATIENT, ELIZABETHGIR DOB: 10/25/2016 00:16 F DOS: 10/25/2016 ATT: MASSEY MD, JULIE S FIN: 77777778 MRN: 101275109	 TESTPATIENT, ELIZABETHGIR DOB: 10/25/2016 00:16 F DOS: 10/25/2016 ATT: MASSEY MD, JULIE S FIN: 77777778 MRN: 101275109
 TESTPATIENT, ELIZABETHGIR DOB: 10/25/2016 00:16 F DOS: 10/25/2016 ATT: MASSEY MD, JULIE S FIN: 77777778 MRN: 101275109	 TESTPATIENT, ELIZABETHGIR DOB: 10/25/2016 00:16 F DOS: 10/25/2016 ATT: MASSEY MD, JULIE S FIN: 77777778 MRN: 101275109	 TESTPATIENT, ELIZABETHGIR DOB: 10/25/2016 00:16 F DOS: 10/25/2016 ATT: MASSEY MD, JULIE S FIN: 77777778 MRN: 101275109

#### **After:**

 TESTPATIENT, ELIZABETHGIRL DOB: 10/25/2016 00:02 F DOS: 10/25/2016 ATT: MASSEY MD, JULIE S FIN: 777777779 MRN: 200000447	 TESTPATIENT, ELIZABETHGIRL DOB: 10/25/2016 00:02 F DOS: 10/25/2016 ATT: MASSEY MD, JULIE S FIN: 777777779 MRN: 200000447	 TESTPATIENT, ELIZABETHGIRL DOB: 10/25/2016 00:02 F DOS: 10/25/2016 ATT: MASSEY MD, JULIE S FIN: 777777779 MRN: 200000447
  TESTPATIENT, ELIZABETHGIRL DOB: 10/25/2016 00:02 F DOS: 10/25/2016 ATT: MASSEY MD, JULIE S FIN: 777777779 MRN: 200000447	 TESTPATIENT, ELIZABETHGIRL DOB: 10/25/2016 00:02 F DOS: 10/25/2016 ATT: MASSEY MD, JULIE S FIN: 777777779 MRN: 200000447	 TESTPATIENT, ELIZABETHGIRL DOB: 10/25/2016 00:02 F DOS: 10/25/2016 ATT: MASSEY MD, JULIE S FIN: 777777779 MRN: 200000447
 TESTPATIENT, ELIZABETHGIRL DOB: 10/25/2016 00:02 F DOS: 10/25/2016 ATT: MASSEY MD, JULIE S FIN: 777777779 MRN: 200000447	 TESTPATIENT, ELIZABETHGIRL DOB: 10/25/2016 00:02 F DOS: 10/25/2016 ATT: MASSEY MD, JULIE S FIN: 777777779 MRN: 200000447	 TESTPATIENT, ELIZABETHGIRL DOB: 10/25/2016 00:02 F DOS: 10/25/2016 ATT: MASSEY MD, JULIE S FIN: 777777779 MRN: 200000447

**ALBERT EINSTEIN HEALTHCARE NETWORK  
POLICY AND PROCEDURE**

**Supersedes:** A0214.1, A0211.2,  
A0271, A0234.2, A0217

**No:** A0214.2

**Date:** December 15<sup>th</sup>, 2016

**Effective Date:** December 15<sup>th</sup>, 2016

**Page 1 of 5**

---

**Department:** Information Services  
**Subject:** Information Security Program

---

**I. PURPOSE**

The purpose of this policy is to define and establish the Einstein Healthcare Network (Einstein) Information Security Program.

**II. POLICY**

The Information Security Program is comprised of the people, policies, procedures, technology, standards, and governance committees that enable Einstein to protect its information and information systems. The Information Security Program supports Einstein's mission by protecting information and information systems and by complying with all applicable laws, regulations and accreditation standards.

**III. Scope**

This policy applies to all Einstein, locations, departments, Workforce Members and users of Einstein systems and networks.

**IV. DEFINITIONS**

Einstein Information: Any data, communication or information created by Workforce Members in the course of their work or created on Information Systems, including but not limited to, paper and electronic documents electronic mail (email), voice mail, faxes, medical records, research data, employee records, and network traffic.

Information System: Any information technology device, network or software owned, leased, or otherwise controlled by Einstein, or used by Workforce Members to access, process, store, transmit or protect Einstein Information. This includes, but is not limited to laptop and desktop computers, software applications, scanners, printers, multipurpose copy devices, smartphones, tablets, servers, databases, fax machines, firewalls, switches, routers, and other network devices.

Workforce Members: Employees, medical staff, students, contractors, consultants, vendors, volunteers, and others affiliated with Einstein, whether or not they are paid by Einstein.

**ALBERT EINSTEIN HEALTHCARE NETWORK  
POLICY AND PROCEDURE**

Supersedes: A0214.1, A0211.2,  
A0271, A0234.2, A0217

No: A0214.2

Date: December 15<sup>th</sup>, 2016

Effective Date: December 15<sup>th</sup>, 2016

Page 2 of 5

---

**Department: Information Services**  
**Subject: Information Security Program**

---

**V. PROCEDURE**

- A. Leadership: Einstein's Chief Information Officer has oversight responsibility for the Information Security Program. The Chief Information Officer appoints a Chief Information Security Officer. The Chief Information Security Officer has primary responsibility for designing and implementing the Information Security Program and will consult with other Einstein departments including, but not limited to, Information Services, Legal, Facilities, Human Resources, Compliance, and operational departments in designing and implementing the Information Security Program.
- B. Participation: All Workforce Members are expected to participate in the Information Security Program by becoming familiar with policies, attending training required by the Information Security Program, and implementing the practices required by the Information Security Program's policies, procedures, and standards in their job duties. While the Information Security Program is led by the Chief Information Security Officer, implementation of the Information Security Program is supported by the efforts of Workforce Members in all areas of Einstein. Examples of implementation activities include, but are not limited to, managing access to systems, conducting background checks, attending training, or implementing secure systems.
- C. Principles: The Information Security Program is guided by a set of core principles:
1. Risk Management: Information security decisions are made based on risk, and risk is assessed as a function of the likelihood and impact of events that may negatively impact Einstein. Decisions around reducing information security risks take into account the costs and benefits of the risk reduction and Einstein's size, complexity and capabilities.
  2. Defense in Depth: Security controls are designed in a layered way such that, where possible, the failure of any individual control does not lead to a loss.
  3. Least Privilege: Workforce members have access to Einstein Information and Information Systems they need to complete their job functions but do not have access to Einstein Information and Information Systems where there is not a job related need.
- D. Information Security Governance: The Information Security Program is monitored and governed by the Information Security and Privacy Oversight Committee. The structure and membership of the Information Security

**ALBERT EINSTEIN HEALTHCARE NETWORK  
POLICY AND PROCEDURE**

Supersedes: A0214.1, A0211.2,  
A0271, A0234.2, A0217

No: A0214.2

Date: December 15<sup>th</sup>, 2016

Effective Date: December 15<sup>th</sup>, 2016

Page 3 of 5

---

**Department: Information Services**  
**Subject: Information Security Program**

---

Committee is defined by the Information Security and Privacy Oversight Committee Charter.

- E. Implementation: When the Information Security Program establishes or modifies a policy or standard, Einstein-wide compliance with that standard is implemented in a reasonable timeframe based on then-existing circumstances, including a risk-based prioritization, the complexity of the technical changes necessitated by the standard, and the costs of the necessary changes.
- F. Information Security Policies and Standards: The Information Security Program is in part defined by information security policies, procedures and standards approved by the Chief Information Officer and Chief Information Security Officer. These policies, procedures and standards apply to all Workforce members.
1. Where a regulation, including, but not limited to HIPAA or HITECH, requires an action, activity or assessment to be documented, Einstein maintains a written record of the action, activity or assessment and retains such documentation for 6 years from the date of its creation or the date when the document last was in effect, whichever is later.
  2. Information security policies will be reviewed at least once every three years to ensure they remain up to date.
- G. Information Security Program Objectives: The Information Security Program focuses on delivering the following:
1. Confidentiality, Integrity and Availability of Information: Einstein's information is accessible only to authorized individuals, is protected from unauthorized modification, and is accessible when needed.
  2. Incident Response: Identifying and responding to information security incidents.
  3. Identity and Access Management: Verifying and managing the identity of Workforce Members and their access to Einstein Information.
  4. Information Security Risk Assessment: Identifying and ranking information security risks and guiding risk owners in making risk treatment decisions.
  5. Documentation: The procedures and standards that create and implement the Information Security Program.



**ALBERT EINSTEIN HEALTHCARE NETWORK  
POLICY AND PROCEDURE**

Supersedes: A0214.1, A0211.2,  
A0271, A0234.2, A0217

No: A0214.2

Date: December 15<sup>th</sup>, 2016

Effective Date: December 15<sup>th</sup>, 2016

Page 4 of 5

---

**Department: Information Services**  
**Subject: Information Security Program**

---

6. Information and Classification and Handling: Categorizing information and information systems in order to facilitate application of appropriate protections.
7. Self-Assessment: Reviewing Einstein's compliance with relevant laws, regulations and accreditation standards and providing guidance on how compliance can be improved.
8. Project and New System Security: Advising projects and other efforts in order to integrate information security smoothly into changes to Einstein information systems and processes.
9. Third Party Risk Management: Assessing the security of information handled by or impacted by third parties.
10. Security Metrics and Reporting: Providing usable information to Einstein's senior management on the state of information security at Einstein.
11. System and Network Security: Protecting Einstein's computer networks and information systems through configuration management, virus and mobile code protection, and other protective measures.
12. Vulnerability Management: Identifying and addressing technical vulnerabilities.
13. Logging and Monitoring: Creating and reviewing records of system activity to identify or discourage policy violations or the compromise of security controls.
14. Physical Security of Information Assets: Implementing measures to prevent unauthorized physical access to Information Assets.
15. Information Security Awareness and Training: Training Workforce Members on their responsibilities and the requirements of the Information Security Program.
16. Sanctions: Identification of non-compliance with the Information Security Program and remedy as described in Einstein's Violations of Information Security and Privacy Policy (*Policy # HR 121.2 Violations of Information Security and Privacy*)

**Violation of Policy**

As defined in Einstein's *Policy # HR 121.2 Violations of Information Security and Privacy*, violations of this policy will be addressed through Einstein's performance

 1A

**ALBERT EINSTEIN HEALTHCARE NETWORK  
POLICY AND PROCEDURE**

Supersedes: A0214.1, A0211.2,  
A0271, A0234.2, A0217

No: A0214.2

Date: December 15<sup>th</sup>, 2016

Effective Date: December 15<sup>th</sup>, 2016

Page 5 of 5

---

**Department: Information Services**  
**Subject: Information Security Program**

---

accountability process (policy # *HR 133 Performance Accountability Program*) and may include sanctions up to and including termination.

**VI. RESPONSIBILITY**

**The Chief Information Security Officer** will provide training and support relating to this policy.

**Einstein Workforce Members** are responsible for knowledge of and compliance with the policy and procedure outlined here.

**Einstein Management** are responsible for the implementation, enforcement and maintenance of this policy and procedure.

**VII. RENEWAL/REVIEW**

This policy is to be reviewed every three years to determine if the policy complies with current regulations. In the event that significant related technology or regulatory changes occur, the policy will be reviewed and updated as needed

**X. APPROVED BY:**

  
\_\_\_\_\_  
Signature

11/16/2016  
\_\_\_\_\_  
Date

**Chief Information Security and Privacy Officer**

  
\_\_\_\_\_  
Signature

11/16/2016  
\_\_\_\_\_  
Date

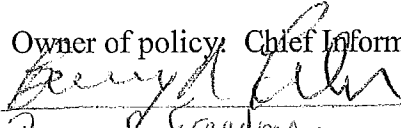
**Chief Information Officer**

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Date

**President and CEO**

Owner of policy: Chief Information Security and Privacy Officer

  
\_\_\_\_\_  
Barry R. Freedman  
President & CEO

12/20/16  
\_\_\_\_\_  
Date

**ALBERT EINSTEIN HEALTHCARE NETWORK  
POLICY AND PROCEDURE**

**Supersedes:** A0270  
**Date:** December 15<sup>th</sup> 2016

**No:** A0270.1  
**Effective Date:** December 15<sup>th</sup> 2016  
**Page 1 of 5**

---

**Department:** Information Services  
**Subject:** Information Classification Policy

---

**I. PURPOSE**

The purpose of this policy is to categorize Einstein Healthcare Network (Einstein) information into categories, called classifications, to enable effective communication about the various types of information in use at Einstein and the protections required for that information.

**II. POLICY**

Einstein Information is any data, communication or information created by Einstein Workforce Members or created on Einstein's Information Systems. Einstein Information is classified as Public Information, Non-Public Information, or Confidential Information, with Public Information requiring the lowest level of security and Confidential Information requiring the highest. In cases where a more granular definition is needed, Confidential Information can be broken down into the categories of Restricted Information, Regulated Information, and Sensitive Information.

These information classification levels are defined as follow:

1. Public Information: Public Information is information that is approved for general distribution outside Einstein. Examples include content on Einstein.edu and press releases.
2. Non-Public Information: Non-Public Information is Einstein Information that is not specifically approved for public release and that does not fall into the category of Confidential Information. Examples of Non-Public Information include voice mails and emails with content that do not fall into another category.
3. Confidential Information: Confidential Information is Einstein Information that requires special protection because loss of the information's confidentiality, availability, or integrity would impair Einstein's ability to achieve its mission. Confidential Information includes the sub categories of Restricted Information, Regulated Information, and Sensitive Information which are defined as follows:
  - a. Restricted Information: Restricted Information is confidential information that requires special protection because loss of the information's confidentiality, availability or integrity would impair Einstein's ability to achieve its mission. Restricted Information includes, but is not limited to:
    - i. Legal: Materials protected by attorney-client privilege, work product as well as information related to ongoing or potential litigation or subject to legal hold.
    - ii. Business Operations: Board meeting minutes, information related to Einstein finances, non-public regulatory filings, audit reports



ALBERT EINSTEIN HEALTHCARE NETWORK  
POLICY AND PROCEDURE

Supersedes: A0270  
Date: December 15<sup>th</sup> 2016

No: A0270.1  
Effective Date: December 15<sup>th</sup> 2016  
Page 2 of 5

---

Department: Information Services  
Subject: Information Classification Policy

---

- and work papers, non-public tax records, and details of unannounced mergers, acquisitions, or restructurings.
- iii. Clinical Operations: Details around the timing, volume, or staffing for sensitive procedures, such as elective termination of pregnancy.
  - iv. Human Resources: Personnel files, payroll and salary information, grievances, lists of aggregated contact or demographic information for Einstein students, faculty or staff, and accident reports.
  - v. Technical Information: Passwords or other passcodes, system configuration details, full descriptions of system vulnerabilities, and encryption keys.
  - vi. Confidential Research Information: Inventions (as defined in the Intellectual Property Policy A0991), trade secrets, copyrightable materials, non-public and other confidential information related to unpublished research results or information related to the management of research animals.
  - vii. Contractually Protected Information: Information covered by contracts or other legal agreements that require the information to be secured or kept confidential.
  - viii. Other Confidential Information: Any information that, if released, may potentially subject Einstein to liability or otherwise cause harm to Einstein, Workforce Members, or the public is considered Restricted Information. Workforce Members are expected to use good professional judgment to identify information that falls into this category.
- b. Regulated Information: Regulated Information is information that requires special protections due to a law, regulation, or accreditation standard. Regulated Information includes:
- i. Protected Health Information (PHI): Any data or information, whether oral or recorded, in any form or medium that identifies or can readily be associated with the identity of a patient or other person and is related to a patient's health status; or is obtained in the course of a patient's health care from a health care provider, from the patient, from a member of a patient's family, or an individual with whom the patient has a close personal relationship, or from the patient's legal representative.



**ALBERT EINSTEIN HEALTHCARE NETWORK  
POLICY AND PROCEDURE**

**Supersedes: A0270  
Date: December 15<sup>th</sup> 2016**

**No: A0270.1  
Effective Date: December 15<sup>th</sup> 2016  
Page 3 of 5**

---

**Department: Information Services  
Subject: Information Classification Policy**

---

- ii. Research Participant Information: Information related to research participants is subject to the same policies and security controls as PHI whether the research participant is a patient of Einstein.
- iii. Personally Identifiable Information (PII): The term Personally Identifiable Information, as defined in the Breach of Personal Information Notification Act 73 P.S. Section 2301 et seq. is an individual's first name or first initial and last name in combination with and linked to any one or more of the following data elements:
  - Social Security number
  - Driver's license number or number of a State identification card number issued in lieu of a driver's license
  - Financial account number, credit or debit card number, in combination with any required security code, access code or password.

The definition of PII includes information related to individuals who are not patients of Einstein.

- iv. Cardholder Data: Cardholder Data is credit card information, as regulated by the Payment Card Industry (PCI) data security standard. Cardholder Data includes credit card numbers, debit card or other payment card numbers, partial credit card or debit card numbers that include more digits than the first six and last four digits, magnetic card stripe data, debit card PINs, and CVV2 codes (the 3 or 4 digit code included on the front or back of a card). If card holder name or card expiration date are stored with the other data elements noted, they are also considered Cardholder Data.
- c. Sensitive Information: Sensitive Information is Protected Health Information (PHI) that requires additional confidentiality controls because there is an unusually high risk of patient harm in the event that the information is disclosed. Sensitive information includes PHI related to:
  - i. Sexually transmitted disease testing or diagnosis, including HIV status
  - ii. Psychiatric notes
  - iii. Mental health diagnosis
  - iv. Drug or alcohol treatment



**ALBERT EINSTEIN HEALTHCARE NETWORK  
POLICY AND PROCEDURE**

**Supersedes:** A0270  
**Date:** December 15<sup>th</sup> 2016

**No:** A0270.1  
**Effective Date:** December 15<sup>th</sup> 2016  
**Page 4 of 5**

---

**Department:** Information Services  
**Subject:** Information Classification Policy

---

**Breach of Policy**

As defined in AEHN's Policy # HR 121.2 Violations of Information Security and Privacy, Workforce Members who violate this and any other Information Security and Privacy policies and procedures are subject to sanctions up to and including termination.

**III. DEFINITIONS**

**Einstein Information:** Any data, communication or information created by Workforce Members in the course of their work or created on Information Systems, including but not limited to, paper and electronic documents electronic mail (email), voice mail, faxes, medical records, research data, employee records, and network traffic.

**Information System:** Any information technology device, network or software owned, leased, or otherwise controlled by Einstein, or used by Workforce Members to process, store, transmit or protect Einstein Information. This includes, but is not limited to laptop and desktop computers, software applications, scanners, printers, multipurpose copy devices, smartphones, tablets, servers, databases, firewalls, switches, routers, and other network devices.

**Workforce Member:** Employees, volunteers, and other persons whose conduct, in the performance of work for Einstein, is under the direct control of Einstein, whether or not they are paid Einstein. This includes full and part time employees, physicians, dentists, affiliates, associates, students, volunteers, and staff not employed by Einstein who provide service to Einstein.

**IV. SCOPE**

This policy applies to all EHN, locations, departments, Workforce Members and users of EHN systems and networks. This policy applies to any and all media, electronic, paper, or otherwise on which the information described by this policy may be held.

**V. RESPONSIBILITY**

**The Chief Information Security and Privacy Officer** will provide training and support relating to this policy.

**Workforce Members** are responsible for knowledge of and compliance with the policy and procedure outlined here.

**Einstein Management** are responsible for the implementation, enforcement and maintenance of this policy and procedure.



ALBERT EINSTEIN HEALTHCARE NETWORK  
POLICY AND PROCEDURE

Supersedes: A0270  
Date: December 15<sup>th</sup> 2016

No: A0270.1  
Effective Date: December 15<sup>th</sup> 2016  
Page 5 of 5

---

Department: Information Services  
Subject: Information Classification Policy

---

**VI. RENEWAL/REVIEW**

This policy is to be reviewed every three years to determine if the policy complies with current regulations. In the event that significant related technology or regulatory changes occur, the policy will be reviewed and updated as needed


**VII. APPROVED BY:**

  
\_\_\_\_\_ 11/16/2016  
\_\_\_\_\_

Chief Information Security and Privacy Officer      Date  
  
\_\_\_\_\_ 11/16/2016  
\_\_\_\_\_

Chief Information Officer      Date

Owner of policy: Chief Information Security and Privacy Officer

  
\_\_\_\_\_ 12/20/16  
Barry R. Freedman  
President & CEO      Date



**ALBERT EINSTEIN HEALTHCARE NETWORK  
POLICY AND PROCEDURE**

Supersedes: A0215.2, A0222.2, A0282, A0245, A0034.3 No: A0222.3  
A0219.2, A0219.2, A0278 A0251.1, A0266.1, A0253.2

Date: December 15, 2016

Effective Date: Dec. 15, 2016

Page 1 of 10

---

**Department: Information Services**

**Subject: Acceptable Use of Information Systems**

---

## **I. PURPOSE**

This policy defines the acceptable use of Einstein's Information and Information Systems.

## **II. POLICY**

Einstein Workforce Members must adhere to the following criteria when making use of Einstein Information and Information Systems:

- A. Ethics and Values: Use of Einstein Information and Information Systems must be in line with Einstein's values as described in the Code of Conduct (Policy HR 135), Einstein GPS Program and Compliance Program (Policy A0228)
- B. Security: Use of Einstein Information and Information Systems must not expose Einstein Information to un-due risk of unauthorized disclosure, modification or deletion.
- C. Productivity: Personal use of Information Systems must not be excessive or interfere with completing job responsibilities.
- D. Legal: Under no circumstances are Einstein Workforce Members authorized to engage in any activity that is illegal or fraudulent under local, state, federal or international law while utilizing Einstein Information or Information Systems. Use of Einstein Information and Information Systems must not place Einstein at risk of legal action.

## **III. DEFINITIONS**

Confidential Information: See the Information Classification Policy (A0270.1) for the full definition of Confidential Information. In brief, Confidential Information is Einstein Information that that requires special protection because loss of the information's confidentiality, availability, or integrity would impair Einstein's ability to achieve its mission. Confidential Information includes patient information, data about employees, and a variety of other types of information as described in the Information Classification Policy.

Einstein Information: Any data, communication or information created by Workforce Members in the course of their work or created on Information Systems, including but not limited to, paper and electronic documents electronic mail (email), voice mail, faxes, medical records, research data, employee records, and network traffic.

Einstein-Owned Device: Any Smartphone or Tablet that is purchased by Einstein or otherwise legally Einstein property that is used to access, process, transmit, or store Confidential Information or access Einstein email. These devices remain with Einstein when the Workforce Member's relationship with Einstein ends.





**ALBERT EINSTEIN HEALTHCARE NETWORK  
POLICY AND PROCEDURE**

Supersedes: A0215.2, A0222.2, A0282, A0245, A0034.3 No: A0222.3  
A0219.2, A0219.2, A0278 A0251.1, A0266.1, A0253.2

Date: December 15, 2016

Effective Date: Dec. 15, 2016

Page 2 of 10

---

**Department: Information Services**

**Subject: Acceptable Use of Information Systems**

---

Personally-Owned Device: Any Smartphone or Tablet that is purchased by a Workforce Member or otherwise legally the Workforce Member's property that is used to conduct Einstein business or access, process, transmit, or store Confidential Information or access Einstein email. These devices remain with the Workforce Member when the Workforce Member's relationship with Einstein ends.

Information System: Any information technology device, network or software owned, leased, or otherwise controlled by Einstein, or used by Workforce Members to access, process, store, transmit or protect Einstein Information. This includes, but is not limited to laptop and desktop computers, software applications, scanners, printers, multipurpose copy devices, smartphones, tablets, servers, databases, fax machines, firewalls, switches, routers, and other network devices.

Smartphone: Any portable wireless phone with data storage capability and the ability to link to and communicate with other electronic devices, software, or the Internet. Examples include iPhones, Windows Phones, Android phones and Blackberries.

Tablet: Any portable computing device based on a mobile operating system with the ability to communicate with the internet. Examples include, but are not limited to, iPads, iPad Minis, Samsung Galaxy devices, iTouch, and Kindle Fire devices. Laptops and MacBooks are not considered to be tablets.

Workforce Members: Employees, medical staff, students, contractors, consultants, vendors, volunteers, and others affiliated with Einstein, whether or not they are paid by Einstein.

## **IV. PROCEDURE**

### **A. General Provisions**

1. Professionalism: Workforce Members are responsible for professional, ethical use of Einstein Information consistent with Einstein's mission and Code of Conduct at all times.
2. Inappropriate Content: Access, download or transmission of pornographic, obscene or sexually explicit material (unless related to a legitimate, documented clinical or academic purposes), racial slurs or similar offensive material is prohibited. This prohibition includes any communication which contains sexual or racial overtones, disparages any individual(s) based on race, sex, age, national origin, religion, sexual orientation and/or any other personal characteristic protected under federal, state or local laws, or which would be inconsistent with Einstein's policies on Equal Employment Opportunity and Sexual Harassment (Policy HR009.4 Equal

 AF

**ALBERT EINSTEIN HEALTHCARE NETWORK  
POLICY AND PROCEDURE**

Supersedes: A0215.2, A0222.2, A0282, A0245, A0034.3 No: A0222.3  
A0219.2, A0219.2, A0278 A0251.1, A0266.1, A0253.2

Date: December 15, 2016

Effective Date: Dec. 15, 2016

Page 3 of 10

---

**Department: Information Services**

**Subject: Acceptable Use of Information Systems**

---

Employment Opportunity and Non Discrimination Policy and Policy HR 077.2  
(Sexual Harassment Policy)

3. Harassment: Workforce Members are prohibited from using Information Systems to harass others whether through language, message content, frequency of communication, size of messages or any other attribute of the communication.
4. Unauthorized Legal Agreements: Workforce Members are prohibited from making legal agreements with third parties related to Einstein business unless authorized according by policy (Policy A0002.2 Signing Authority Policy). This prohibition includes agreeing to End User License Agreements (EULAs) or other agreements required by websites or software vendors.
5. Business Need: Access to Einstein Information is prohibited unless there is a job related need for access. Workforce Members' capability to access Einstein Information does not imply permission or business need to access Einstein Information when it is not required to complete a job related task. For example, a Workforce Member is not allowed to access the medical record of a patient unless access is required for the care of the patient.
6. Security and Privacy Training: Workforce Members are required to complete security and privacy training materials at the start of their relationship with Einstein, during annual compliance training, and when requested. Workforce Members are also expected to participate in security and privacy training and read security and emails and alerts sent from the Chief Information Security and Privacy Officer.

**B. Ownership, Monitoring and Privacy**

1. Ownership: Einstein Information is owned by Einstein unless otherwise specified by Einstein policy, such as the Intellectual Property Policy (Policy A0099.2 Research and Technology Development Policy)
2. Privacy: There is no reasonable expectation of privacy for Workforce Members for any information stored, processed, accessed or transmitted on Einstein's Information Systems, including, but not limited to, photographs, text messages, instant messages, location data, documents, contact information, notes, or other personal data. There is no reasonable expectation of privacy for Workforce Members for Einstein Information stored, processed, accessed or transmitted on Personally-Owned Devices. There may be circumstances where personal data stored on Personally-Owned Devices is accessed inadvertently by Einstein.

**ALBERT EINSTEIN HEALTHCARE NETWORK  
POLICY AND PROCEDURE**

Supersedes: A0215.2, A0222.2, A0282, A0245, A0034.3 No: A0222.3  
A0219.2, A0219.2, A0278 A0251.1, A0266.1, A0253.2

Date: December 15, 2016

Effective Date: Dec. 15, 2016

Page 4 of 10

---

**Department: Information Services**

**Subject: Acceptable Use of Information Systems**

---

3. Monitoring: Einstein may monitor or audit Information Systems at any time. Use of Einstein's Information Systems is considered consent to such monitoring. Einstein reserves the right to override passwords and/or codes and to conduct auditing to ensure compliance with all applicable policies.
4. Authorization for Non-Routine Access: Except for routine monitoring or access for administrative purposes, access without the knowledge and permission of the Workforce Member requires the authorization of a Human Resources director or their designee.
5. Investigations: Workforce Members must cooperate in Einstein investigations. Cooperation includes answering questions, providing requested documentation, providing access to Einstein-Owned and Personally Owned devices, or allowing the device(s) and any Einstein Information on them to be accessed or purged if required by Einstein. Investigations may include, but are not limited to Human Resources, Internal Audit, Legal, Compliance, Information Security and Privacy investigations.

### **C. Compliance**

1. Accreditations, Certifications and Titles: Workforce Members must adhere to all accreditation standards and certification requirements that apply to Einstein or to professional certifications or titles held by the Workforce Member.
2. Intellectual Property Law: Violations of the rights of any person or organization protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, are prohibited. This includes, but is not limited to:
  - a. Installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Einstein Workforce Members.
  - b. Unauthorized copying and or distribution of copyrighted material including, but not limited to, music, movies, texts, and/or photographs.

### **D. Personal Use of Einstein Information**

1. Personal Use: Incidental use of Einstein's Information Systems for personal reasons is permitted provided that such usage is on personal time, has supervisory permission, does not put the interests of Einstein at risk and does not conflict with the provisions of this, or other Einstein policies. Einstein departments may establish their own guidelines and rules that restrict or otherwise further limit internet access or other personal use of Information Systems

**ALBERT EINSTEIN HEALTHCARE NETWORK  
POLICY AND PROCEDURE**

Supersedes: A0215.2, A0222.2, A0282, A0245, A0034.3 No: A0222.3  
A0219.2, A0219.2, A0278 A0251.1, A0266.1, A0253.2

Date: December 15, 2016

Effective Date: Dec. 15, 2016

Page 5 of 10

---

**Department: Information Services**

**Subject: Acceptable Use of Information Systems**

---

2. Personal Data Storage: Incidental storage of personal information on Einstein Information Systems is permitted, however Workforce Members must be aware that personal data may be deleted or lost as part of system maintenance, upgrades, or failures. Storage of large volumes of personal data, such as pictures, videos or other files is not permitted and any such files may be deleted from Einstein systems without notice. Personal data on Einstein systems may be viewed at any time by Einstein as noted in section B.2. Personal data stored on Einstein Information Systems may be unavailable to Workforce Members after their relationship with Einstein ends.

#### **E. Information Security and Privacy**

1. Report Information Security or Privacy Incidents: Workforce Members must report suspected or known information security or privacy incidents by notifying the Information Security or Privacy Officer or calling the Help Desk at 215-456-8033 or anonymously by calling the ComplyLine at 1-866-458-4864. Examples of information security or privacy incidents include:
  - a. PHI mailed or faxed to the wrong recipient
  - b. Lost or stolen medical records, or other files containing PHI
  - c. Inappropriate verbal discussion of PHI where the conversation was overheard
  - d. Receiving suspicious e-mail
  - e. Two Workforce Members sharing an account or password
  - f. An Einstein website with unusual or unexpected content
  - g. Lost or stolen portable devices such as iPhones, laptops, thumb drives, or other media
  - h. Placing paper documents that contain PHI in the regular trash
  - i. Any other violation of information security policies
2. Password Sharing: Workforce Members are responsible for the security of their passwords and are accountable for all actions taken using their account and password. Revealing your Einstein account passwords to others or allowing use of your Einstein accounts or by others is prohibited. This prohibition includes family and other household members as well as other Einstein Workforce Members.
3. Screen Lock: Workforce Members are responsible for locking the screen of their computer when it is not in use.

**ALBERT EINSTEIN HEALTHCARE NETWORK  
POLICY AND PROCEDURE**

Supersedes: A0215.2, A0222.2, A0282, A0245, A0034.3 No: A0222.3  
A0219.2, A0219.2, A0278 A0251.1, A0266.1, A0253.2

Date: December 15, 2016

Effective Date: Dec. 15, 2016

Page 6 of 10

---

**Department: Information Services**

**Subject: Acceptable Use of Information Systems**

---

4. Update System Access: Workforce Members with management responsibility are required follow access management procedures and immediately update PRISM when any Workforce Member they manage changes job role or exits their relationship with Einstein.
5. Physically Secure Portable Devices: Information stored on laptops, smartphones and other portable devices is especially vulnerable to theft or loss. Workforce Members must take precautions to avoid losing devices or leaving devices unattended in an insecure location such as a vehicle or conference room.
6. Unauthorized Devices: Placing Einstein data on unauthorized devices or connecting unauthorized devices to the Einstein network is prohibited. Unauthorized devices connected to Einstein networks or Information Systems may be confiscated or disconnected without notice.
7. Personal Computers: Workforce Members are not permitted to download Einstein data onto non-Einstein owned computers, tablets, smartphones or other similar devices unless the device is managed by Einstein or otherwise approved for use by the IS department. Use of remote access tools such as virtual desktops, web pages, and email from non-Einstein computers is permitted as long as data is not downloaded and stored locally on the computer.
8. Bypassing Security Controls: Workforce Members are prohibited from engaging in activity that weakens, disrupts, bypasses or attempts to bypass the security controls around Einstein's Information. Examples of prohibited activities include, but are not limited to:
  - a. Accessing or attempting to access data of which the Workforce is not an intended recipient, user or owner;
  - b. Attempting to or actually accessing another user's account;
  - c. Network sniffing, packet spoofing, or forging routing information for malicious purposes;
  - d. Interfering with or denying service to any Information or individual (for example, denial of service attacks);
  - e. Modifying or creating information with the intent to mislead or deceive, for example, modifying email header information or system logs;
  - f. Introduction of malicious programs into the Einstein network or any Einstein server or computer (e.g., viruses, worms, Trojan horses, etc.); and

**ALBERT EINSTEIN HEALTHCARE NETWORK  
POLICY AND PROCEDURE**

Supersedes: A0215.2, A0222.2, A0282, A0245, A0034.3 No: A0222.3  
A0219.2, A0219.2, A0278 A0251.1, A0266.1, A0253.2

Date: December 15, 2016

Effective Date: Dec. 15, 2016

Page 7 of 10

---

**Department: Information Services**

**Subject: Acceptable Use of Information Systems**

---

- g. Port scanning or other security scanning without prior approval from the Enterprise Information Security Officer.

Employees are exempt from these requirements if they are performing a defined job responsibility, such as an Information Services employee accessing another user's account for trouble shooting or conducting network discovery with a port scanner.

#### **F. Email**

1. Professionalism: Workforce Members are expected to maintain a professional approach and adhere to Einstein's Communication Guidelines policy (A0014) when using Einstein email.
2. Personal Email Accounts: Workforce Members must send and receive all emails related to Einstein business using the Einstein email system. Use of personal email accounts to transmit or store Einstein related email is prohibited. Workforce Members are prohibited from sending Einstein business related emails to other Workforce Member's personal email addresses. Workforce Members can identify Einstein email addresses by seeing that an email address ends with @einstein.edu. Contractors, research collaborators, students, non-Einstein-employed residents, and other similar Workforce Members not directly employed by Einstein are permitted to use their employer or school's email account in lieu of an Einstein email account.
3. Mass Emails and "Reply All": Workforce Members are prohibited from sending email to a group where the recipients do not have a need to receive the message in question. This includes "replying all" to a message that was originally sent in error.
4. Phishing: Workforce Members must be aware of "phishing" attacks and take care to avoid them. Phishing attacks are when someone sends an email to a Workforce Member under a false pretense in an attempt to have the Workforce Member reveal their password by responding to the email or clicking on a link.
  - a. Phishing attacks can be emails that look like they come from Einstein or another trusted party. Remember, Einstein will never ask workforce members for their password.
  - b. Most phishing attacks will come from addresses that do not end in "@einstein.edu". Workforce Members should exercise additional care when a message purports to be from Einstein, but does not come from an @einstein.edu address.
  - c. Workforce Members should keep in mind that viruses can send email messages from a compromised account and some websites can install a virus

ALBERT EINSTEIN HEALTHCARE NETWORK  
POLICY AND PROCEDURE

Supersedes: A0215.2, A0222.2, A0282, A0245, A0034.3 No: A0222.3  
A0219.2, A0219.2, A0278 A0251.1, A0266.1, A0253.2

Date: December 15, 2016

Effective Date: Dec. 15, 2016

Page 8 of 10

---

Department: Information Services

Subject: Acceptable Use of Information Systems

---

without requiring the Workforce Member to do anything other than visit the site. Because of this, Workforce Members should never click on unexpected links or attachments even from people the Workforce Member knows.

- d. Workforce Members must immediately report suspected Phishing attacks by calling the Help Desk at 215-456-8033 and by forwarding the message to [reportspam@einstein.edu](mailto:reportspam@einstein.edu) for review.
5. Spam: Workforce Members are prohibited from using Einstein email, or any other email system, to send unsolicited advertisements, also known as spam. Unsolicited advertisements are prohibited in all cases, including advertisements for Einstein services or events. Workforce Members must not use email to solicit or to advocate for non-Einstein or purely personal interests.
6. Email Encryption and Limitations: Einstein email provides email encryption features. Workforce Members must be aware that email encryption only protects emails while they travel across the internet, but does not provide protection to email saved in the sent folder, saved on any device (such as thumb drives) or email once it is delivered. Einstein email utilizes technology that encrypts emails that contain certain types of Protected Health Information ("PHI"). See, Definition of PHI referenced in the Information Classification Policy (Policy A0270.1). This means that even though Einstein email automatically encrypts PHI containing emails:
  - a. Minimum Necessary Information: Workforce Members may only send Confidential Information via email when necessary, and that only the minimum amount of information that is needed to complete a task should be sent. For example, is patient name is not needed in order to describe an issue, do not include patient name in the email.
  - b. Secure Devices: Workforce Members may only send email that contains Confidential Information, such as PHI, from Einstein managed or approved computers, smartphones or tablets or via the Einstein email webpage.
  - c. No PHI in Email Subject Line: PHI such as social security number, patient name or initials, diagnosis, medical record number or other Confidential Information must not be placed in the subject line of emails. The subject line of email is not protected by encryption as the message travels over the internet and subject lines can be observed by someone other than the intended recipient of the message.
  - d. Encryption Keyword: A keyword is available to allow Workforce Members to ensure an email message is encrypted if desired. Workforce Members may



**ALBERT EINSTEIN HEALTHCARE NETWORK  
POLICY AND PROCEDURE**

Supersedes: A0215.2, A0222.2, A0282, A0245, A0034.3 No: A0222.3  
A0219.2, A0219.2, A0278 A0251.1, A0266.1, A0253.2

Date: December 15, 2016

Effective Date: Dec. 15, 2016

Page 9 of 10

---

**Department: Information Services**

**Subject: Acceptable Use of Information Systems**

---

include the word "confidential" in the subject line of an email and the contents of the email will be encrypted.

7. Access to Other User's Email Accounts: Access to another user's email account, often referred to as delegate or proxy access, may be granted only under the following conditions:
  - a. One user grants access to another user in the course of their work
  - b. A user's manager requests access to a former Workforce Member's account
  - c. A user is out of the office for an extended period of time, generally greater than a week, and access is needed by another user to support business functions
  - d. Any other circumstance deemed appropriate by a Human Resources director

#### **G. Instant Messages and Text Messages**

1. Approved Instant Messaging Applications: Workforce Members must only use approved instant messaging applications to communicate Confidential Information. The Einstein Help Desk at 215-456-8033 can provide information on which instant messaging applications are approved. In the case of communication to/from research subjects, communication via text message is acceptable as long as it is consented to by the research subject as part of the research protocol.
2. Secure Texting: Workforce Members may only use approved secure messaging applications to send text messages or instant messages that contain Confidential Information. Workforce Members may not send regular text messages (i.e., SMS messages) or pages that contain Confidential Information. The Einstein Help Desk at 215-456-8033 can provide information on which secure texting applications are approved.
3. Messaging and Medical Records: If an instant message or text message discussion includes content that would be recorded in a medical record if the discussion took place in person or over the phone, follow the same procedure and update the medical record with the details of the discussion.

#### **V. SCOPE**



**ALBERT EINSTEIN HEALTHCARE NETWORK  
POLICY AND PROCEDURE**

Supersedes: A0215.2, A0222.2, A0282, A0245, A0034.3 No: A0222.3  
A0219.2, A0219.2, A0278 A0251.1, A0266.1, A0253.2

Date: December 15, 2016

Effective Date: Dec. 15, 2016

Page 10 of 10

---

**Department: Information Services**  
**Subject: Acceptable Use of Information Systems**

---

This policy applies to all Einstein, locations, departments, Workforce Members and users of Einstein systems and networks.

**VI. RESPONSIBILITY**

**The Chief Information Security and Privacy Officer** will provide training and support relating to this policy.

**Einstein Workforce Members** are responsible for knowledge of and compliance with the policy and procedure outlined here.

**Einstein Management** are responsible for the implementation, enforcement and maintenance of this policy and procedure.

**VII. RENEWAL/REVIEW**

This policy is to be reviewed every three years to determine if the policy complies with current regulations. In the event that significant related technology or regulatory changes occur, the policy will be reviewed and updated as needed

**X. APPROVED BY:**

  
\_\_\_\_\_

Signature

**Chief Information Security and Privacy Officer**

11/16/2016  
\_\_\_\_\_

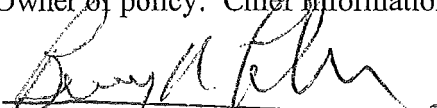
Date

  
\_\_\_\_\_

Signature

**Chief Information Officer**

Owner of policy: Chief Information Security and Privacy Officer

  
\_\_\_\_\_

Barry R. Freedman  
President & CEO

11/16/2016  
\_\_\_\_\_

Date

12/20/16  
\_\_\_\_\_

Date

**ALBERT EINSTEIN HEALTHCARE NETWORK  
POLICY AND PROCEDURE**

Supersedes: NA  
Date: 9/30/16

No: A301  
Effective Date: 9/30/16  
Page 1 of 6

---

**Department: Information Services**  
**Subject: Smartphone and Tablet Security Policy**

---

**I. PURPOSE**

This policy details the security requirements for smartphones and tablets used to handle Einstein Healthcare Network (Einstein) information.

**II. POLICY**

Only approved, secured smartphones and tablets are allowed to access, process, transmit or store Confidential Information or access Einstein email. Smartphones and Tablets must be used by Einstein Workforce Members in a manner that is consistent with applicable regulations, accreditation standards, laws and Einstein policy.

**III. Scope**

This policy applies to all Einstein, locations, departments, Workforce Members and users of Einstein systems and networks.

This policy applies to Smartphones and Tablets used to conduct Einstein business with Confidential Information, approved for Einstein business purposes or used to access, process, transmit, or store Confidential Information (as defined in the Information Classification Policy), whether the device is Personally-Owned or Einstein-Owned.

**IV. DEFINITIONS**

Einstein-Owned Device: Any Smartphone or Tablet that is purchased by Einstein or otherwise legally Einstein property that is used to access, process, transmit, or store Confidential Information or access Einstein email. These devices remain with Einstein when the Workforce Member's relationship with Einstein ends.

Personally-Owned Device: Any Smartphone or Tablet that is purchased by a Workforce Member or otherwise legally the Workforce Member's property that is used to conduct Einstein business or access, process, transmit, or store Confidential Information or access Einstein email. These devices remain with the Workforce Member when the Workforce Member's relationship with Einstein ends.

Non-Exempt Employee: An employee whose assignment does not meet the tests for exemption and who is therefore subject to the minimum wage and overtime provisions of the Fair Labor Standards Act or one who does meet the test for exemption but whom management has voluntarily classified as non-exempt.

Smartphone: Any portable wireless phone with data storage capability and (the ability to link to and communicate with other electronic devices, software, or the Internet. Examples include iPhones, Windows Phones, Android phones and Blackberries.



ME

**ALBERT EINSTEIN HEALTHCARE NETWORK  
POLICY AND PROCEDURE**

Supersedes: NA  
Date: 9/30/16

No: A301  
Effective Date: 9/30/16  
Page 2 of 6

---

**Department: Information Services**  
**Subject: Smartphone and Tablet Security Policy**

---

Tablet: Any portable computing device based on a mobile operating system with the ability to communicate with the internet. Examples include iPads, iPad Minis, Samsung Galaxy devices, iTouch, and Kindle Fire devices. Laptops and MacBooks are not considered to be tablets.

Workforce Members: Employees, medical staff, students, contractors, consultants, vendors, volunteers, and others affiliated with Einstein, whether or not they are paid by Einstein.

## V. PROCEDURE

A. General Provisions: The following provisions apply to the use of Smartphones and Tablets:

1. Data Ownership: Einstein information and data processed or stored on a Personally-Owned Device remains Einstein property at all times.
2. Privacy: There is no reasonable expectation of privacy for Workforce Members for any information stored, processed, accessed or transmitted on Einstein-Owned Devices, including, but not limited to, photographs, text messages, instant messages, location data, documents, contact information, notes, or other personal data. There is no reasonable expectation of privacy for Workforce Members for Einstein-related information stored, processed, accessed or transmitted on Personally-Owned Devices. There may be circumstances where personal data stored on personal devices is accessed inadvertently by Einstein.
3. Restrictions on Access: The content of emails, text messages, pictures, or the phone's location will not be accessed by Einstein without the Workforce Member's knowledge unless there is a legitimate business need. Any access to data stored on an Einstein-Owned Device or Personally-Owned Device without a workforce member's approval requires the approval of a Human Resources director or their designee.
4. Access to Location Information: Before accessing geographic location information for any device through mobile device management software, Information Systems must obtain authorization from the Workforce Member or a Human Resources director or their designee.
5. Procurement: All Einstein-Owned Devices must be procured through IS. Exemptions to this process must be approved by the CIO.

  
NP

**ALBERT EINSTEIN HEALTHCARE NETWORK  
POLICY AND PROCEDURE**

**Supersedes:** NA  
**Date:** 9/30/16

**No:** A201  
**Effective Date:** 9/30/16  
**Page 3 of 6**

---

**Department:** Information Services  
**Subject:** Smartphone and Tablet Security Policy

---

6. Departmental Policy: Workforce must obey departmental policies that do not contradict this policy. For example, if a department establishes a policy that smartphones may not be used during work hours, then that departmental policy must be followed in addition to this policy.
7. Non-Exempt Employees: There is not an expectation that Non-Exempt Employees use Smartphones or Tablets to work out side of their schedule hours. If there is a need for a Non-Exempt Employee to use a Smartphone or Tablet to work outside of scheduled hours, the employee's manager must with a Human Resources director or their designee to address the specific situation.
8. Security Standards: Einstein-Owned or Personally-Owned devices must adhere to published Einstein security standards. Security standards may establish requirements including, but not limited to, specific device types, vendors, software versions, configurations, passwords, or wireless carrier contracts.
9. Device Management: Personally-Owned and Einstein-Owned Devices must have Einstein's mobile device management software application(s) installed on them and must comply with the requirements enforced by those applications. Mobile device management software has the capability to manage device settings and to securely remove data. Workforce Members must not attempt to bypass or actually bypass the controls enforced by these applications.
10. Technical Support: Only Einstein provided hardware, software and applications will be supported by Information Systems. The level of support will be determined by Information Systems and may be limited.
11. Device Assignment: Einstein-Owned Devices assigned to an individual may not be passed off to other individuals for their use without following Information Systems procedures for transferring the device between Workforce Members. Workforce Member's department must collect Einstein-Owned Devices when a Workforce Member's relationship with Einstein ends.
12. Phone Number Transfer: Telephone numbers associated with Einstein-Owned Devices may not be transferred to a Personally-Owned Device when a Workforce Member's relationship with Einstein ends without CIO approval.
13. Diagnostic Images: Workforce Members may not use a Smartphone or Tablet to view medical images for diagnostic purposes unless the device and software are specifically FDA approved for medical image viewing. If

  
1/0

**ALBERT EINSTEIN HEALTHCARE NETWORK  
POLICY AND PROCEDURE**

**Supersedes:** NA  
**Date:** 9/30/16

**No:** R30A  
**Effective Date:** 9/30/16  
**Page 4 of 6**

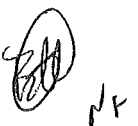
---

**Department:** Information Services  
**Subject:** Smartphone and Tablet Security Policy

---

specifically authorized by departmental procedures, Smartphones and Tablets may be used to view medical images to confirm a diagnosis made by a Workforce Member using a separate FDA approved image viewing device.

14. Cloud Storage and File Sharing Application: Applications that store data on unapproved systems (i.e., cloud storage applications or file sharing applications such as DropBox or iCloud) are not permitted to be used to store or backup Einstein information. Einstein information stored in an encrypted security container application is exempt from this requirement.
  15. Jailbreaking/Rooting: Modified operating system software that bypasses device controls to elevate Workforce Member's permissions or make changes to the device (a.k.a. rooting or jail breaking) must not be used.
  16. Data Removal: If the Workforce Member separates from Einstein, or otherwise exits their relationship with Einstein, an Einstein-Owned or Personally-Owned Device may be completely wiped. Personally-Owned and Einstein-Owned Devices may also be wiped if they are lost, stolen, or otherwise leave the control of the Workforce Member. Einstein is not liable for damage to the device, applications, or data caused by the secure data removal process. Where possible, Einstein will use a selective wipe to only remove Einstein email and data from phones when a wipe is required.
  17. Einstein Liability: Einstein is not liable for any damages or losses to Personally-Owned Devices or data stored or accessed on Smartphones or Tablets.
  18. Location Services: Location services are recommended to be enabled on Smartphones and Tablets in order to allow Mobile Device Management software to determine the location of a lost or stolen device. (Note that as above, access to location information without Workforce Member authorization requires approval from a Human Resources director or their designee.)
- B. Workforce Member Responsibilities: Workforce Members using Einstein-Owned or Personally-Owned devices must adhere to the following:
1. Report Lost or Stolen Devices: In the event an Einstein-Owned or Personally-Owned Device is lost or stolen, Workforce must immediately notify Information Systems by calling the Help Desk at 215-456-8033 so that Einstein information can be removed from the device.



ALBERT EINSTEIN HEALTHCARE NETWORK  
POLICY AND PROCEDURE

Supersedes: NA  
Date: 9/30/16

No: A301  
Effective Date: 9/30/16  
Page 5 of 6

---

Department: Information Services  
Subject: Smartphone and Tablet Security Policy

---

2. Devices Leaving Personal Control: If a Personally-Owned Device will leave the control of the Workforce Member (i.e., Workforce Member wishes to sell, recycle, trade in, or gift the device), Workforce Members must immediately notify Information Systems by calling the Help Desk at 215-456-8033 so that Einstein information can be removed from the device.
  3. Backups: Workforce Members are responsible for performing backups of their Personally-Owned or Einstein-Owned Device. If the backup is done to a personally owned computer, the computer must be maintained in a physically secure location. If a Workforce Member's relationship with Einstein ends or the device that stores the backup is leaving the Workforce Member's possession, the Workforce Member is required to delete the encrypted backup.
  4. Backup Encryption: Backup files created for Personally-Owned and Einstein-Owned Devices must be encrypted and protected with a password.
  5. Physically Secure Devices: Workforce Members must physically secure their Einstein-Owned or Personally-Owned Device by storing them in a secure, locked location, such as an office or desk drawer when the device is not in the Workforce Member's possession, and must not leave devices unattended (for example, do not leave devices in a parked vehicle or conference room).
  6. Phone Number Registration: Workforce Members must register their Personally-Owned Device's phone number with Einstein when requested and must keep this information up to date.
  7. Investigations: Workforce Members must cooperate in investigations by providing access to Einstein-Owned and Personally Owned devices, or allowing the device(s) and any information on them to be accessed or purged if required by Einstein. Investigations may include, but are not limited to human resources, audit, legal, compliance, information security and privacy investigations.
  8. Inappropriate Software: Workforce Members are prohibited from installing or using software, applications or other tools on Smartphones or Tablets to enable or hide violations of this policy or other Einstein policies.
- C. Exemptions: If a portion of this policy cannot or should not be met, discuss with Information Security. An exemption can be approved if a documented, rational justification supports the decision not to meet the standard.

  
MF

ALBERT EINSTEIN HEALTHCARE NETWORK  
POLICY AND PROCEDURE

Supersedes: NA  
Date: 9/30/16

No: A301  
Effective Date: 9/30/16  
Page 6 of 6

---

Department: Information Services  
Subject: Smartphone and Tablet Security Policy

---

**Violation of Policy**

As defined in Einstein's *Policy # HR 121.2 Violations of Information Security and Privacy*, violations of this policy will be addressed through Einstein's performance accountability process (policy # *HR 133 Performance Accountability Program*) and may include sanctions up to and including termination.

**VI. RESPONSIBILITY**

**The Chief Information Security and Privacy Officer** will provide training and support relating to this policy.

**Einstein Workforce Members** are responsible for knowledge of and compliance with the policy and procedure outlined here.

**Einstein Management** are responsible for the implementation, enforcement and maintenance of this policy and procedure.


**VII. Renewal/Review**


This policy is to be reviewed every three years to determine if the policy complies with current regulations. In the event that significant related technology or regulatory changes occur, the policy will be reviewed and updated as needed

**VIII. Related References and Policies**

*Policy # HR 121.2 Violations of Information Security and Privacy*  
*Policy # HR 133.2 Performance Accountability Program*

**IX. Approved By:**

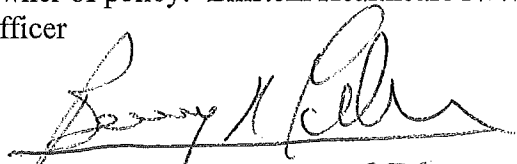
  
\_\_\_\_\_  
Signature

  
\_\_\_\_\_  
Signature

9/19/2016  
\_\_\_\_\_  
Date

9/22/2016  
\_\_\_\_\_  
Date

Owner of policy: Einstein Healthcare Network Chief Information Security and Privacy Officer

  
\_\_\_\_\_  
Barry Freedman, CEO

11/7/16  
\_\_\_\_\_  
Date