

## **HIPAA Privacy Frequently Asked Questions**

### **1. What is HIPAA?**

HIPAA stands for the Health Insurance Portability and Accountability Act of 1996. The privacy rule is contained in the Administrative Simplification mandates of HIPAA. (Another part of HIPAA contains rules regarding pre-existing condition limitations and special enrollment rights.)

The privacy mandates of HIPAA were designed in part to reduce healthcare costs by standardizing the electronic processing of healthcare claims. These mandates include standards for electronic transmission of data and security standards. When Congress enacted these provisions, it recognized that the increased electronic exchange of information that would result from these requirements would in turn give rise to the need for additional privacy protections. Thus, the HIPAA privacy rule was imposed.

### **2. What is the HIPAA privacy rule?**

The privacy rule prohibits health plans from using or disclosing Protected Health Information (“PHI”) except as authorized by the individual who is the subject of the PHI or as explicitly required or permitted by the HIPAA privacy regulations. Additionally, when PHI is used or disclosed, the amount of information must be the minimum necessary to accomplish the purpose of the use or disclosure (the “minimum necessary standard”).

### **3. What is PHI?**

PHI (or protected health information) is health information that is maintained or transmitted by a health plan, (whether oral, written or electronic communication) which identifies the individual to whom the information relates and relates to the individual’s health condition or health treatment.

Examples of documents containing PHI include (i) an explanation of benefits with claims information; (ii) a completed health flexible spending account reimbursement form; (iii) a pharmacy receipt with prescription name; (iv) an email or other document containing (a) the participant’s name and (b)(1) medical condition, (2) services received or (3) physician bills.

### **4. Who is covered by the HIPAA privacy rule?**

The privacy rule applies to health plans, providers, and healthcare clearinghouses. For our purposes, HIPAA applies to us because BAE SYSTEMS sponsors a health plan that is subject to HIPAA.

HIPAA applies to employers only indirectly through the group health plan it sponsors. This explains why documents, like the notice of privacy practice and the policies and procedures adopted for HIPAA, are from and refer to the BAE SYSTEMS health plans, rather than BAE SYSTEMS as a company.

### **5. What is a “health plan” for purposes of HIPAA?**

“Group health plan” means medical, dental, vision, prescription drug, health flexible spending account plans, and employee assistance plans.

Disability plans, life insurance, workers compensation and family and medical leave administration are not subject to HIPAA. While those plans and programs are not subject to HIPAA, BAE SYSTEMS requires that you treat correspondence and documentation for those plans and programs with the same high level of strict confidentiality.

### **6. When must I obtain a participant’s authorization?**

If you need to use or disclose the participant’s protected health information, you must first obtain the participant’s written authorization. The participant must sign and date the authorization form. Once completed, you must fax the completed authorization form to:

Privacy Officer  
c/o BAE SYSTEMS BenefitCenter  
Fax (856) 770-3412<sup>1961</sup>

**7. When must I obtain a spouse's authorization?**

Spouses and employees have independent rights. This means that if you disclose an employee's PHI to the employee's spouse, you must obtain the employee's written authorization.

Similarly, if you disclose a spouse's PHI to an employee, you must obtain the spouse's written authorization.

**8. Where can I find an authorization form?**

Go to [www.na.baesystems.com/benefits](http://www.na.baesystems.com/benefits) or <http://BAESYSTEMS.benefitcenter.com> for an authorization form.

**9. Once the issue is resolved, where do I file the information I acquired in order to assist the employee?**

Once the issue is resolved, there is no need to retain the information you acquired when assisting the employee. You must shred all documents and notes that contain PHI. If you believe the information you have should be retained by the plan, please contact the Privacy Officer.

**10. Who is the privacy officer?**

Steve Epstein, VP of Compensation, Benefits and HRIS

**11. Where should I refer a participant's inquiries and complaints regarding his/her privacy rights?**

The participant should write to:

Privacy Officer  
c/o BAE SYSTEMS BenefitCenter  
P.O. Box 4846  
Chesapeake, VA 23327-4846  
Fax (856) 770-3412

**12. What is the minimum necessary standard?**

The minimum necessary standard requires that you disclose only the minimum amount of PHI necessary to accomplish the intended purpose of the use, disclosure or request.

For example, assume John P. Smith asks his HR representative to assist with determining what blood pressure medications are covered under the plan. HR representative calls a benefit representative for assistance. In explaining, the request to benefits representative, the HR representative states "John P. Smith has been diagnosed with high blood pressure and wants to know what medications are covered by the plan."

HR representative's disclosure to the benefit representative is a violation of the minimum necessary standard. In order to accomplish his/her objective, the HR representative did not need to provide the name and diagnosis of the individual seeking assistance.

**13. What are the penalties for failing to comply with the requirements of HIPAA?**

- a. Workforce Sanctions. If you violate the policies and procedures of the plan, you will be subject to workforce sanctions, including HIPAA re-training and/or disciplinary action, including termination.
- b. Civil Penalties. Your violation of the plan's policies and procedures could result in a civil penalty of \$100 per violation, up to \$25,000 for each violation in a single year. This penalty will apply even if the violation is accidental or inadvertent.
- c. Criminal Penalties. For intentional wrongful disclosures, you are subjecting yourself to a \$50,000 fine and up to 1 year in jail. If the wrongful disclosure is made under false pretenses, the penalty may include up to a \$100,000 fine and up to 5 years in jail. If the disclosure is made with malicious intent, the penalty may include up to a \$250,000 fine and up to 10 years in jail.