






# Compliance and Security Update








MHBE Governing Board  
April 17, 2017

MARYLAND  
HEALTH BENEFIT  
EXCHANGE



# MARYLAND HEALTH BENEFIT EXCHANGE

Audits Q1 into Q2 2017	Status	Comments
Independent External Audit – Financial PY16		Finding related to invoicing oversight and approval process. Procedure under review. All PY2015 findings cleared.
Independent External Audit – Programmatic PY16		QHP decertification procedures that comply with 45 CFR 155.1080 (b) and address segregation of duties, roles, and responsibilities implemented. Termination of QHP enrollment to be automated. PY16 Audit to begin April 17, 2017.
Privacy Impact Assessment PY16 and MARS-E v 2.0		Design, revise and implement new Privacy Controls section of the Minimum Acceptable Risk Standards for State-based Exchanges (MARSE v2.0) by June 30, 2017 to Include internal controls related to : <ul style="list-style-type: none"> <li>• Authority and Purpose to Collect PII</li> <li>• Accountability, Audit and Risk Management</li> <li>• Data, Quality and Integrity</li> <li>• Data Minimization and Retention</li> <li>• Individual Participation and Redress</li> <li>• Security</li> <li>• Transparency</li> <li>• Use Limitation</li> </ul>
Audit Preparation FY2017		<ul style="list-style-type: none"> <li>• GAO Eligibility and Enrollment on-site review February 23-24, 2017</li> <li>• Independent External Audit PY 2016 Programmatic – April 17</li> <li>• IRS 1075 Safeguards – May 23-25, 2017</li> <li>• State –Based Marketplace Annual Reporting Tool (SMART) PY 16 – June 1, 2017</li> <li>• Office of Legislative Audit – Anticipated June</li> <li>• Privacy Impact Assessment – June 30, 2017</li> </ul>
Fraud, Waste and Abuse Reporting		YTD 6 reported incidents. (2) referred to DHMH OIG. No investigations found FWA.

Authority to Connect requirements for 2017 Summary	Status	Comments
Annual Security and Privacy Attestation	N/A	Not required for 2017. An independent Security Assessment Report will be generated this year in 2018 and will address security and privacy for years 1, 2, and 3.
Privacy Impact Assessment (PIA)		Completed last Privacy Impact Assessment along with Privacy team and received completed PIA mitigation closure from CMS on 9/20/2016. Opened findings and added to Agency Plan of Action and Milestones (POA&M). Next PIA due June 30 <sup>th</sup> .
Information Security Risk Assessment (ISRA)		The MARS-E Risk Assessment addresses: next ISRA due with ATC submission <ul style="list-style-type: none"> <li>Assurance of Confidentiality, Integrity, and Availability (CIA) of the system</li> <li>Effectiveness of implemented security and privacy controls</li> <li>Foreseeable internal and external threats to the information</li> <li>Likelihood of the threats exploiting on vulnerabilities</li> <li>Sufficiency of policies and procedures to mitigate the threats</li> </ul>
Plan of Action and Milestones (POA&M)		Completed Quarter 1 POA&M, Quarter 2 POA&M due April 28 th,2017.
IRS Safeguard Security Report (SSR)		Completed Annual SSR, The SSR addresses all outstanding Actions identified by the IRS from prior years submissions. Next SSR due May 31, 2017.
IRS Corrective Action Plan (CAP)	✓ Complete	No CAP presently due because CAP was closed with IRS
System Security Plan (SSP)		Update System Security Plan to MARS-E 2.0 compliance. MARS-E 2.0 is the latest security standard required for state based exchanges. Target date: May 30 <sup>th</sup> , 2017.
Security Assessment Report (SAR)		Plan, Procure and deliver Third Party independent assessment of System Security Plan, Security and Privacy Controls consistent with the MARS-E 2.0. The triennial security and privacy control testing necessary for the renewal of an Authority to Connect (ATC). Target date: August 30 <sup>th</sup> ,2017.
Authority to Connect		Deliver Authority to Connect Package: includes System Security Plan (SSP), Security Assessment Report (SAR), Plan of Action & Milestones (POA&M), Signed Associate Information Security Agreement (ISA), Interconnection Security Agreement (ISA). Target Date: November 6, 2017