6/1/23 Discussion Draft

205 CMR 257: SPORTS WAGERING DATA PRIVACY

257.01: Definitions

As used in 205 CMR 257.00, the following words and phrases shall have the following meanings, unless the context clearly indicates otherwise:

Data Breach means Breach of Security as that phrase is defined in M.G.L. c. 93H, § 1.

Confidential Information means information related to a Sports Wagering Account, the placing of any Wager or any other sensitive information related to the operation of Sports Wagering including the amount credited to, debited from, withdrawn from, or present in any particular Sports Wagering Account; the amount of money Wagered by a particular patron on any event or series of events; the unique patron ID or username and authentication credentials that identify the patron; the identities of particular Sporting Events on which the patron is Wagering or has Wagered, or the location from which the patron is Wagering, has Wagered, or has accessed their Sports Wagering Account. Confidential Information may also include Personally Identifiable Information.

Personally Identifiable Information means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular patron, individual or household. Personally Identifiable Information includes, but is not limited to, Personal Information as that phrase is defined in M.G.L. c. 93H and 201 CMR 17.00. Personally Identifiable Information may also include Confidential Information.

257.02: Data Use and Retention

(1) A Sports Wagering Operator shall only use Confidential Information and Personally Identifiable Information as necessary to operate a Sports Wagering Area, Sports Wagering Facility or Sports Wagering Platform, or to comply with M.G.L. c. 23N, 205 CMR, or any other applicable law, regulation, court order, subpoena or civil investigative demand of a governmental entity.

(2) If a Sports Wagering Operator seeks to use a patron's Confidential Information or Personally Identifiable Information for purposes beyond those specified in 257.02(1), a Sports Wagering Operator shall obtain the patron's consent, which may be withdrawn at any time.

(a) Such consent must be clear, conspicuous, and received apart from any other agreement or approval of the patron. Acceptance of general or broad terms of use or similar documents that purport to permit the sharing of Confidential Information or Personally Identifiable Information in the same

document shall not constitute adequate consent, nor shall hovering over, muting, pausing, pre-selecting, or closing a given piece of content without affirmative indication of consent.

(b) Consent shall not be deemed to be a waiver of any of the patron's other rights.

(c) The option to withdraw such consent must be clearly and conspicuously available to the patron on the Sports Wagering Operator's Sports Wagering Platform. A patron shall not be required to confirm withdrawal of consent more than once, and no intervening pages or offers will be presented to the patron before such confirmation is presented to the patron.

(3) A Sports Wagering Operator may not use a patron's Personally Identifiable Information or Confidential Information, or any information derived from it, to promote or encourage specific wagers or promotional offers based on:

(a) a period of dormancy or non-use of a Sports Wagering Platform;

(b) the wagers made or promotional offers accepted by other patrons with a known or predicted social connection to the patron;

(c) the communications of the patron with any third party other than the Operator;

(d) the patron's actual or predicted

i. income, debt, net worth, credit history, or status as beneficiary of governmental programs;

ii. medical status or conditions; or

iii. occupation.

(e) Any computerized algorithm, automated decision-making, machine learning, artificial intelligence, or similar system that is known or reasonably expected to make the gaming or sports wagering platform more addictive.

(4) A Sports Wagering Operator shall only retain a patron's Confidential Information and Personally Identifiable Information as necessary to operate a Sports Wagering Area, Sports Wagering Facility or Sports Wagering Platform or to comply with M.G.L. c. 23N, 205 CMR, or any other applicable law, regulation, court order, subpoena or civil investigative demand of a governmental entity.

(5) A Sports Wagering Operator shall collect and aggregate patrons' Confidential Information and Personally Identifiable Information to analyze patron behavior for the purposes of identifying and developing programs and interventions to promote

responsible gaming and support problem gamblers, and to monitor and deter Sports Wagering in violation of G.L. c. 23N and 205 CMR. The Sports Wagering Operator shall provide a report to the Commission at least every six months on the Sports Wagering Operator's compliance with this subsection, including the trends observed in this data and the Sports wagering Operator's efforts to mitigate potential addictive behavior.

257.03: Data Sharing

(1) A Sports Wagering Operator shall not share a patron's Confidential Information or Personally Identifiable Information with any third party except as necessary to operate a Sports Wagering Area, Sports Wagering Facility or Sports Wagering Platform or to comply with M.G.L. c. 23N, 205 CMR, or any other applicable law, regulation, court order, subpoena, or civil investigative demand of a governmental entity.

(2) If a Sports Wagering Operator shares a patron's Confidential Information or Personally Identifiable Information pursuant to 257.03(1), the Operator shall take commercially reasonable measures to ensure the party receiving a patron's Confidential Information or Personally Identifiable Information keeps such data private and confidential, except as required to comply with M.G.L. c. 23N, 205 CMR, or any other applicable law, regulation, court order, subpoena, or civil investigative demand of a governmental entity. The party receiving such data shall only use a patron's Confidential Information or Personally Identifiable Information for the purpose(s) for which the data was shared.

(3) If a Sports Wagering Operator deems it necessary to share a patron's Confidential Information or Personally Identifiable Information with a Sports Wagering Vendor, Sports Wagering Subcontractor, or Sports Wagering Registrant in order to operate its Sports Wagering Area, Sports Wagering Facility or Sports Wagering Platform or to comply with M.G.L. c. 23N, 205 CMR, any other applicable law, regulation, court order, subpoena, or civil investigative demand of a governmental entity, a Sports Wagering Operator shall enter into a written agreement with the Sports Wagering Vendor, Sports Wagering Subcontractor or Sports Wagering Registrant, which shall include, at a minimum, the following obligations:

(a) The protection of all Confidential Information or Personally Identifiable Information that may come into the third party's custody or control against a Data Breach;

(b) The implementation and maintenance of a comprehensive data-security program for the protection of Confidential Information and Personally Identifiable Information, which shall include, at a minimum, the following:

i. A security policy for employees relating to the storage, access and transportation of Confidential Information or Personally Identifiable Information;

ii. Restrictions on access to Personally Identifying Information and Confidential Information, including the area where such records are kept, secure passwords for electronically stored records and the use of multi-factor authentication;

iii. A process for reviewing data security policies and measures at least annually; and

iv. An active and ongoing employee security awareness program for all employees who may have access to Confidential Information or Personally Identifiable Information that, at a minimum, advises such employees of the confidentiality of the data, the safeguards required the protect the data and any applicable civil and criminal penalties for noncompliance pursuant to state and federal law.

(c) The implementation, maintenance, and update of security and breach investigation and incident response procedures that are reasonably designed to protect Confidential Information and Personally Identifiable Information from unauthorized access, use, modification, disclosure, manipulation or destruction; and

(d) A requirement that the maintenance of all Confidential Information and Personally Identifiable Information by a Vendor, Subcontractor or Registrant must meet the standards provided in 257.03.

(4) Sports Wagering Operators shall encrypt and protect, including through the use of multi-factor authentication, from incomplete transmission, misrouting, unauthorized message modification, disclosure, duplication or replay all Confidential Information and Personally Identifiable Information.

257.04: Patron Access

(1) Patrons shall be provided with a method to make the requests in 205 CMR 257.04(a)-(e). The request must be clearly and conspicuously available to the patron online through the Sports Wagering Operator's Sports Wagering Platform. A patron shall not be required to confirm their request more than once, and no intervening pages or offers will be presented to the patron before such confirmation is presented to the patron.

(a) A description as to how their Confidential Information or Personally Identifiable Information is being used, including confirmation that such Confidential Information or Personally Identifiable Information is being used in accordance with this Section 205 CMR 257;

(b) Access to a copy of their Confidential Information or Personally Identifiable Information maintained by the Operator or a Vendor, Subcontractor, or Registrant of the Operator;

(c) Updates to their Confidential Information or Personally Identifiable Information;

(d) The imposition of additional restriction on the use of their Confidential Information or Personally Identifiable Information for particular uses; and

(e) That their Confidential Information or Personally Identifiable Information be erased when it is no longer required to be retained by applicable law or Court order.

(2) A Sports Wagering Operator shall provide a written response to a request submitted pursuant to 257.04(1) that either grants or denies the request.

(a) If the Sports Wagering Operator grants the patron's request to access a copy of their Personally Identifiable Information, the Sports Wagering Operator shall provide the patron their Confidential Information or Personally Identifiable Information in a structured, commonly used and machine readable format.

(b) If the Sports Wagering Operator denies the request, the Sports Wagering Operator shall provide in its written response specific reason(s) supporting the denial and directions on how the patron may file a complaint regarding the denial with the Commission.

(3) A Sports Wagering Operator shall grant the patron's request to impose a restriction or erase their Confidential Information or Personally Identifiable Information if:

(a) It is no longer necessary to retain the patron's Confidential Information or Personally Identifiable Information to operate a Sports Wagering Area, Sports Wagering Facility or Sports Wagering Platform, or to comply with M.G.L. c. 23N, 205 CMR, or any other applicable law, regulation, court order, subpoena or civil investigative demand of a governmental entity;

(b) The patron withdraws their consent to the Sports Wagering Operator's retention of their Confidential Information or Personally Identifiable Information;

(c) There is no overriding legal interest to retaining the patron's Confidential Information or Personally Identifiable Information;

(d) The patron's Confidential Information or Personally Identifiable Information was used in violation of 205 CMR 257.00; or

(e) Restriction or erasure is necessary to comply with an order from the Commission or a court.

(4) If the Sports Wagering Operator grants the patron's request to erase their Confidential Information or Personally Identifiable Information, the Sports

Wagering Operator shall erase the patron's Personally Identifiable Information or Confidential from all storage media it is currently using to operate a Sports Wagering Area, Sports Wagering Facility or Sports Wagering Platform, including HDD, SDD, flash, mobile, cloud, virtual, RAID, LUN, hard disks, solid state memory, and other devices. The Sports Wagering Operator shall also request confirmation of deletion from any Vendor, Registrant, or Subcontractor who received the patron's Confidential Information or Personally Identifiable Information from the Sports Wagering Operator. Notwithstanding, the foregoing, the Sports Wagering Operator shall not erase a patron's Confidential Information or Personally Identifiable Information on backup or storage media used to ensure the integrity of the Sports Wagering Area, Sports Wagering Facility or Sports Wagering Platform from technology failure or to comply with its data retention schedule or to comply with M.G.L. c. 23N, 205 CMR, or any other applicable law, regulation, court order, subpoena or civil investigative demand of a governmental entity.

(5) An Operator, or a Vendor, Registrant or Subcontractor of an Operator shall not require a Patron to enter into an agreement waiving any of the Patron's rights under this Section 257.

257.05: Data Program Responsibilities

(1) A Sports Wagering Operator shall develop, implement and maintain comprehensive administrative, technical and physical data privacy and security policies appropriate to the size and scope of business and addressing, at a minimum:

(a) Practices to protect the confidentiality, integrity and accessibility of Confidential Information or Personally Identifiable Information;

(b) The secure storage, access and transportation of Confidential Information or Personally Identifiable Information, including the use of encryption and multi-factor authentication;

(c) The secure and timely disposal of Confidential Information or Personally Identifiable Information, including data retention policies;

(d) Employee training on data privacy and cybersecurity for employees who may have access to Confidential Information or Personally Identifiable Information that, at a minimum, advises such employees of the confidentiality of the data, the safeguards required the protect the data and any applicable civil and criminal penalties for noncompliance pursuant to state and federal law;

(e) Restrictions on access to Personally Identifying Information or Confidential Information, including the area where such records are kept, secure passwords for electronically stored records and the use of multi-factor authentication;

(f) Reasonable monitoring of systems, for unauthorized use of or access to Confidential Information or Personally Identifying Information;

(g) Reasonably up-to-date versions of system security agent software which must include malware protection and reasonably up-to-date patches and virus definitions, or a version of such software that can still be supported with up-to-date patches and virus definitions, and is set to receive the most current security updates on a regular basis;

(h) Cybersecurity insurance, which shall include, at a minimum, coverage for data compromise response, identity recovery, computer attack, cyber extortion and network security;

(i) Data Breach investigation and incident response procedures;

(j) Imposing disciplinary measures for violations of Confidential Information and Personally Identifiable Information policies;

(k) Active oversight and auditing of compliance by Vendors, Registrants, or Subcontractors with 257.03(3) and with the Operator's Confidential Information and Personally Identifying Information policies.

(l) Quarterly information system audits; and

(m) A process for reviewing and, if necessary, updating data privacy policies at least annually.

(2) A Sports Wagering Operator shall maintain on its website and Sports Wagering Platform a readily accessible copy of a written policy explaining to a patron the Confidential Information and Personally Identifiable Information that is required to be collected by the Sports Wagering Operator, the purpose for which Confidential Information or Personally Identifiable Information is being collected, the conditions under which a patron's Confidential Information or Personally Identifiable Information may be disclosed, and the measures implemented to otherwise protect a patron's Confidential Information or Personally Identifiable Information. A Sports Wagering Operator shall require a patron to agree to the policy prior to collecting any Confidential Information or Personally Identifiable Information, and require a patron to agree to any material updates. Agreement to this policy shall not constitute required consent for any additional uses of information.

(3) A Sports Wagering Operator, Sports Wagering Vendor, Sports Wagering Subcontractor, Sports Wagering Registrant, or Person to whom an Occupational License is issued shall comply with all applicable state and federal requirements for data security, including M.G.L. c. 93A, M.G.L. c. 93H, 940 CMR 3.00, 940 CMR 6.00 and 201 CMR 17.00.

257.06: Data Breaches

(1) In the event of a suspected Data Breach involving a patron's Confidential Information or Personally Identifiable Information, a Sports Wagering Operator shall immediately notify the Commission and commence an investigation of the suspected Data Breach, which shall be completed in no more than five (5) days from the discovery of the suspected breach.

(2) Following completion of the investigation specified pursuant to 257.06(1), the Sports Wagering Operator shall submit a written report to the Commission describing the suspected Data Breach and stating whether any patron's Confidential Information or Personally Identifying Information was subjected to unauthorized access. Unless the Sports Wagering Operator shows that unauthorized access did not occur, the Sports Wagering Operator's written report shall also detail the Operator's plan to remediate the Data Breach, mitigate its effects, and prevent Data Breaches of a similar nature from occurring in the future.

(3) Upon request by the Commission, the Sports Wagering Operator shall provide a report from a qualified third-party forensic examiner, the cost of which shall be borne by the Sports Wagering Operator being examined.

(4) In addition to the other provisions of this 205 CMR 257.06, the Sports Wagering Operator shall be required to comply with any other legal requirements applicable to such Data Breaches or suspected Data Breaches, including its obligations pursuant to G.L. c. 93H and 201 CMR 17.00.